PELS RIJCKEN

Landsadvocaat

De inzet van slimme technologie in voetbalstadions voor de aanpak van discriminatie en racisme

Een verkenning van het juridisch speelveld

Sandra van Heukelom-Verhage, Gerrit-Jan Zwenne, Nina Bontje en Tim Gillhaus

18 mei 2021

Inhoudsopgave

1	INLEIDING	6
1.1	*Aanleiding en reikwijdte van de verkenning*	*6*
1.2	*Aanpak en bronnen*	*7*
1.3	*Leeswijzer*	*8*
2	MANAGEMENTSAMENVATTING	10
2.1	*Samenvatting en conclusie*	*10*
2.2	*De keuzeladder*	*13*
2.2.1	Fase 1 − Signaleren van discriminatie en racisme	13
2.2.2	Fase 2 − Identificeren van de betrokkene	19
2.2.3	Fase 3 − Gebruik van de gegevens ten behoeve van sanctieoplegging	22
2.3	*Tot slot*	*26*
DEEL 1		31
3	DE INZET VAN SLIMME TECHNOLOGIEËN: EEN INTRODUCTIE	32
3.1	*Mogelijke technologieën per fase*	*32*
3.1.1	Fase 1 − Signaleren van discriminatie en racisme	32
3.1.2	Fase 2 − Identificeren van de betrokkene	35
3.1.3	Fase 3 − Gebruik van de gegevens ten behoeve van sanctieoplegging	37
3.2	*Betrokken partijen*	*38*
3.3	*Onderscheid verschillende camera's*	*40*
4	TOEPASSELIJKHEID VAN DE AVG: WORDEN ER PERSOONSGEGEVENS VERWERKT?	41
4.1	*Juridisch kader*	*41*
4.1.1	Materieel toepassingsgebied: het verwerken van persoonsgegevens	41
4.1.2	Anonieme gegevens en gepseudonimiseerde persoonsgegevens	41
4.1.3	Bijzondere persoonsgegevens	43
4.1.4	Strafrechtelijke persoonsgegevens	44
4.1.5	Wanneer is sprake van een verwerking (van persoonsgegevens)?	46
4.1.6	Zijstap: sectorale gegevensbeschermingswetten	46
4.2	*De verwerking van persoonsgegevens met de slimme technologieën in voetbalstadions*	*47*
4.2.1	Fase 1 − Signaleren van discriminatie en racisme	47
4.2.2	Fase 2 − Identificeren van de betrokkene	51
4.2.3	Fase 3 − Gebruik van de gegevens ten behoeve van sanctieoplegging	52
4.2.4	Tot slot: toepasselijkheid Wpg en Wjsg	53

5	WIE VERWERKEN PERSOONSGEGEVENS?	55
5.1	*Juridisch kader*	*55*
5.1.1	De verwerkingsverantwoordelijke	55
5.1.2	Gezamenlijke verwerkingsverantwoordelijken	55
5.1.3	(Sub)verwerkers	56
5.2	*Kwalificatie van de betrokken partijen*	*57*
5.2.1	Fase 1 − Signaleren van discriminatie en racisme	57
5.2.2	Fase 2 − Identificeren van de betrokkene	58
5.2.3	Fase 3 − Gebruik van de gegevens ten behoeve van sanctieoplegging	59
6	GRONDSLAGEN, NOODZAKELIJKHEID EN DOELBINDING	60
6.1	*Juridisch kader*	*60*
6.1.1	Wettelijke grondslag	60
6.1.2	Noodzakelijkheidsbeginsel	64
6.1.3	Doelbinding en verdere verwerkingen	66
6.1.4	Uitzonderingsgronden voor bijzondere persoonsgegevens, waaronder biometrie	67
6.1.5	Uitzonderingsgronden voor strafrechtelijke persoonsgegevens	72
6.2	*Grondslagen voor de onderhavige verwerkingen?*	*72*
6.2.1	Fase 1 − Signaleren van discriminatie en racisme	72
6.2.2	Fase 2 − Identificeren van de betrokkene	81
6.2.3	Fase 3 − Gebruik van de gegevens ten behoeve van sanctieoplegging	87
7	GEAUTOMATISEERDE BESLUITVORMING EN PROFILERING	97
7.1	*Juridisch kader*	*97*
7.2	*Aandachtspunten bij de inzet van slimme technologieën*	*100*
DEEL 2		103
8	OVERIGE JURIDISICHE VOORWAARDEN VOOR DE INZET VAN SLIMME TECHNOLOGIEËN	104
8.1	*Inleiding*	*104*
8.2	*Internationale doorgifte*	*104*
8.3	*Rechtmatige, behoorlijke en transparante verwerking & non-discriminatiebeginsel*	*105*
8.4	*Juistheidsbeginsel*	*111*
8.5	*Beginsel van opslagbeperking*	*112*
8.6	*Beveiliging*	*112*
8.7	*De verantwoordingsplicht*	*115*
8.8	*De meldplicht datalekken*	*115*
8.9	*Data Protection Impact Assessment (DPIA)*	*116*
9	TRANSPARANTIE EN RECHTEN VAN BETROKKENEN	118

9.1 Inleiding 118
9.2 Het recht op informatie 118
9.3 Het recht op inzage 122
9.4 Het recht op rectificatie 123
9.5 Het recht op gegevenswissing 123
9.6 Het recht op beperking van de verwerking (artikel 18 AVG) 124
9.7 Het recht op dataportabiliteit 125
9.8 Het recht op bezwaar 125
9.9 Uitzonderingen op de rechten van de betrokkene 126

DISCLAIMER 128

BIJLAGE 1 129

BIJLAGE 2 134

BIJLAGE 3 136

BEGRIPPENLIJST

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BSN	Burgerservicenummer
Bjsg	Besluit justitiële en strafvorderlijke gegevens
BVO	Betaaldvoetbalorganisatie
CNIL	Commission nationale de l'informatique et des libertés
DPIA	Data protection impact assessment
EDPB	European Data Protection Board
HvJ	Hof van Justitie van de Europese Unie
KNVB	Koninklijke Nederlandse Voetbalbond
KVV	Keten Voorziening Voetbal
OM	Openbaar Ministerie
OVIVI	Ons Voetbal Is Van Iedereen
SyRI	Systeem Risico Indicatie
TTP	Trusted Third Party
UAVG	Uitvoeringswet AVG
Wbp	Wet bescherming persoonsgegevens
Wpg	Wet politiegegevens
Wjsg	Wet justitiële en strafvorderlijke gegevens

1 INLEIDING

1.1 Aanleiding en reikwijdte van de verkenning

Aanleiding van deze verkenning vormt het aanvalsplan Ons Voetbal Is Van Iedereen – samen zetten we racisme en discriminatie buitenspel ('OVIVI'). Dat betreft een gezamenlijk plan van de Rijksoverheid, de Koninklijke Nederlandse Voetbalbond ('KNVB'), de Eredivisie en de Keuken Kampioen Divisie om discriminatie en racisme in het voetbal te voorkomen, signaleren en aanpakken.[1]

Een van de maatregelen uit het aanvalsplan is het beschikbaar maken en inzetten van slimme technologie in voetbalstadions. Om daders van racistisch en/of discriminatoir gedrag in voetbalstadions aan te pakken, wordt onderzocht of betaaldvoetbalorganisaties ('**BVO's**') met behulp van slimme technologie beter vast kunnen gaan leggen wie zich binnen een stadion schuldig maakt aan racistische of discriminerende uitingen. Dit zou de BVO's, de KNVB en het Openbaar Ministerie ('OM') beter in staat moeten stellen (civiel- dan wel strafrechtelijk) tegen deze personen op te treden.[2] Momenteel wordt onderzocht of de inzet van slimme technologieën een bijdrage kan leveren aan de signalering, identificatie en aanpak (sanctieoplegging) van discriminatie en racisme.

In dat kader is eerder reeds een marktverkenning uitgevoerd naar de (technische) mogelijkheden om (combinaties van) slimme technologie te ontwikkelen die de signalering, identificering en aanpak van personen die zich schuldig maken aan discriminatie en racisme in het voetbalstadion mogelijk maakt. Uit deze marktverkenning volgt dat door verschillende technologische oplossingen te combineren (zoals de inzet van bepaalde opnameapparatuur en gezichts- en stem/spraakherkenningstoepassingen), het mogelijk lijkt te zijn een technologie te ontwikkelen waarmee personen kunnen worden geïdentificeerd die zich in stadions schuldig maken aan racistische en discriminerende uitingen.

Tegelijkertijd roept de inzet van deze (combinatie van) slimme technologie de vraag op of en zo ja, hoe deze technologie kan worden ingezet in overeenstemming met privacywet- en regelgeving.

Dit rapport is het resultaat van een verkennend onderzoek naar de privacyrechtelijke kaders voor de inzet van slimme technologieën in voetbalstadions, met als doel het signaleren en aanpakken van discriminatie en racisme. In dat kader is onderzocht of en zo ja, hoe slimme technologie kan worden ingezet in overeenstemming met de Algemene Verordening Gegevensbescherming ('AVG'), de Uitvoeringswet AVG ('UAVG') en eventuele bijzondere gegevensbeschermingswet- en regelgeving die van toepassing is.

---

1 Zie daarover https://onsvoetbalisvaniedereen.nl/.
2 Zie p. 22 van het aanvalsplan.

Daarnaast wordt in dit rapport middels een sanctiekaart inzichtelijk gemaakt welke civielrechtelijke en strafrechtelijke mogelijkheden het slachtoffer, de BVO's en de KNVB hebben om (door middel van de op basis van slimme technologie vastgestelde incidenten) op te treden tegen discriminatie of racisme.

1.2 Aanpak en bronnen

Ten behoeve van dit onderzoek hebben wij allereerst een kick-offbijeenkomst gehouden met betrokken medewerkers van het Ministerie van VWS, Sportinnovator en de KNVB.

Vervolgens hebben wij interviews afgenomen met de volgende stakeholders:

1. Sjoerd Griffioen en Rutger Spierenburg (KNVB)
   Tijdens dit interview is gesproken over de privacyrechtelijke aandachtspunten en risico's die bij de KNVB bekend zijn. Daarbij is ook stil gestaan bij de bestaande verwerkingen, de waarborgen die door de stadions en de KNVB reeds zijn getroffen, de onderlinge rollen en verantwoordelijkheden en de omvang van de problematiek.

2. Floor Waardenburg en Niels Reijgersberg (Sportinnovator), gelijktijdig met Leonard Ariëns en Alexander Josiassen (NewBizz)
   Tijdens dit interview is gesproken over de (marktverkenning naar) slimme technologieën die kunnen worden ingezet ten behoeve van het signaleren en aanpakken van personen die zich schuldig maken aan discriminatie of racisme. Geïnventariseerd is welke slimme technologieën reeds worden toegepast en/of reeds zijn onderzocht, hoe deze technologieën werken en hoe deze kunnen bijdragen aan het signaleren en aanpakken van discriminatie en racisme.

3. Leo Vellekoop (veiligheidscoördinator bij ADO Den Haag)
   Tijdens dit interview is besproken hoe BVO's, en meer specifiek ADO Den Haag, op dit moment maatregelen treffen om discriminatoir en racistisch gedrag te signaleren, de betrokkenen te identificeren en de betrokkenen vervolgens aan te pakken. Daarbij is ook stilgestaan bij de onderlinge rolverdeling tussen de BVO's, de KNVB, gemeente, politie en het OM. Voorts is gesproken over de uitdaging bij het signaleren, identificeren en aanpakken, en bij de vraag in hoeverre de inzet van slimme technologie daarvoor een oplossing kan bieden.

4. Jan Willem van Dop (algemeen directeur bij Go Ahead Eagles)
   Tijdens dit interview is eveneens gesproken over hoe BVO's, en meer specifiek Go Ahead Eagles, op dit moment maatregelen treffen om discriminatoir en racistisch gedrag te signaleren, de betrokkenen te

identificeren en de betrokkenen vervolgens aan te pakken. Daarbij is ook stilgestaan bij de wenselijkheid van de inzet van slimme technologie en bij de bredere problematiek van discriminatie en racisme in het voetbal.

5. John A.J.M. Riemen en Joost Arents (beiden werkzaam bij de politie en specialist in de inzet van biometrie)
Tijdens dit interview is gesproken over de inzet van slimme technologieën (waaronder biometrie) bij de signalering, identificatie en aanpak van daders. Ook is gesproken over de bestaande samenwerking tussen de BVO's, de KNVB, de politie en het OM op dit vlak.

Voorts is het noodzakelijke juridische desk-onderzoek uitgevoerd. Daarvoor zijn onder andere de relevante rechtspraak en rapporten van de privacytoezichthouder(s) geïnventariseerd en bestudeerd.

1.3 Leeswijzer

Dit rapport bestaat uit twee delen.

Deel 1 bevat het privacyrechtelijke kader voor de inzet van slimme technologieën in voetbalstadions ter signalering van en sanctieoplegging voor discriminatie en racisme. Dit kader passen wij daarbij toe op de slimme technologieën die centraal staan in dit rapport.

Dit deel wordt voorafgegaan door een managementsamenvatting waarin de belangrijkste conclusies worden toegelicht en in beeld worden gebracht (hoofdstuk 2). In de hoofdstukken 3 tot en met 7 worden deze conclusies uitgewerkt.

Daartoe lichten wij eerst de slimme technologieën toe die centraal staan in dit rapport, evenals de partijen die bij de inzet daarvan betrokken zullen zijn (hoofdstuk 3).

Vervolgens zetten wij het relevante privacyrechtelijke kader uiteen voor de beoordeling van de toelaatbaarheid van de inzet van deze slimme technologieën (hoofdstuk 4 t/m 7). Daarbij toetsen wij of de verschillende slimme technologieën (kunnen) voldoen aan de eisen die uit dat kader volgen. Het gaat achtereenvolgend om:

- De vraag of (bijzondere) persoonsgegevens worden verwerkt en de AVG (dus) van toepassing is (hoofdstuk 4);
- De vraag wie ten aanzien van deze verwerkingen de verwerkingsverantwoordelijke of de (sub)verwerker is (hoofdstuk 5);
- De grondslag, noodzaak en doelbinding van die verwerkingen, evenals de aanwezigheid van uitzonderingsgronden voor de verwerking van bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens (hoofdstuk 6). Wij

lichten onze conclusies daarbij toe aan de hand van een fictieve casus (zie hoofdstuk 6.2).

- Het verbod op geautomatiseerde besluitvorming, waaronder profilering (hoofdstuk 7).

Daarbij wordt aan de hand van de reeds geïnventariseerde slimme technologieën geïllustreerd hoe de privacyrechtelijke beoordeling van in te zetten slimme technologieën dient plaats te vinden, en concluderen wij ten aanzien van de reeds geïnventariseerde slimme technologieën wat op dit moment vanuit privacyrechtelijk oogpunt mogelijk is (zie hoofdstuk 2). Eventuele andere slimme technologieën die in de toekomst worden overwogen om in te zetten, zullen aan eenzelfde beoordeling moeten worden onderworpen.

Deel 2 bevat de (overige) gegevensbeschermingsrechtelijke voorwaarden waaraan de inzet van slimme technologieën in voetbalstadions moet voldoen (hoofdstuk 8). Daarbij gaan wij ook in op de transparantieverplichting en de rechten van betrokkenen (hoofdstuk 9).

2 MANAGEMENTSAMENVATTING

In dit rapport staat de vraag centraal of slimme technologie kan worden ingezet in voetbalstadions om discriminatie en racisme aan te pakken. Meer specifiek gaat het om de vraag hoe die inzet van slimme technologie zich verhoudt tot de (U)AVG en eventuele andere gegevensbeschermingswetten.

2.1 Samenvatting en conclusie

De aanpak van discriminatie en racisme met behulp van slimme technologie valt uiteen in drie fases:

(1) Allereerst moet discriminatoir of racistisch gedrag worden gesignaleerd en vastgelegd; de zgn. signaleringsfase. Deze fase eindigt op het moment dat beelden zijn geselecteerd waaruit (een vermoeden van) discriminatoir of racistisch gedrag blijkt;
(2) Daarna moeten degenen die betrokken zijn bij dat discriminatoire of racistische gedrag (de mogelijke "daders") worden geïdentificeerd; de zgn. identificatiefase; en
(3) Tot slot moeten de daadwerkelijk bij het gewraakte gedrag aan de betrokkenen een sanctie worden opgelegd; de zgn. sanctiefase.

Hoewel deze drie fases met elkaar samenhangen en in elkaars verlengende liggen, zal de inzet van slimme technologie in ieder van deze fases een ander doel dienen (namelijk: signaleren, identificeren of aanpakken/sanctie opleggen). Deze verschillende doeleinden moeten worden onderscheiden om te kunnen beoordelen of de inzet van slimme technologie in ieder van deze fases toelaatbaar is.

Daarnaast moet onderscheid worden gemaakt tussen de verschillende slimme technologieën die kunnen worden ingezet. Het gaat in dit rapport hoofdzakelijk om beeld- en geluidopnameapparatuur (camera's met microfoons) die technologisch vooruitstrevende functionaliteiten bevatten. Wij maken daarbij onderscheid tussen:

- De 'gewone' camera; dat zijn de videocamera's die gewoonweg beeldopnames maken, zoals beveiligingscamera's. Soms maken dit soort camera's ook geluidsopnames. De inzet van 'gewone' camera's is op dit moment al verplicht in stadions van BVO's op grond van de licentie-eisen van de KNVB;
- De slimme camera; dat zijn camera's die in staat zijn om op basis van beeld- en geluidopnames discriminatoir of racistisch gedrag te herkennen, daarop in te zoomen en vervolgens dat gedrag zowel in beeld als geluid vastleggen; en
- De camera met gezichtsherkenningstechnologie; dat zijn camera's die in staat zijn om op basis van een beeldopname (en soms ook/mede op basis van een geluidopname) van een persoon de betreffende persoon kunnen identificeren. De camera maakt daarbij door middel van gezicht- en/of

stemherkenningstechnologie een vergelijking tussen de persoon die wordt gefilmd en eerder verkregen referentiemateriaal.

Aan de hand van dit kader zijn wij tot de volgende conclusie gekomen:

Signaleringsfase - Tijdens een voetbalwedstrijd kunnen slimme camera's worden ingezet die discriminatoir of racistisch gedrag signaleren en vastleggen. Als de noodzaak voor de inzet van deze slimme camera's met slimme microfoons kan worden onderbouwd en ook overigens kan worden voldaan aan de eisen die in de (U)AVG worden gesteld, achten wij dit een rechtmatig gebruik van slimme technologie in voetbalstadions. De inzet van deze slimme technologie **– de zgn. slimme camera's –** in de signaleringsfase is dan toelaatbaar. Een belangrijke kanttekening is dat niet valt uit te sluiten dat met de inzet van slimme technologie strafrechtelijke persoonsgegevens worden verwerkt. Daarvan is sprake als de opnames een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren. Het verdient aanbeveling om met de Autoriteit Persoonsgegevens ('AP') in gesprek te gaan of het noodzakelijk is om voor deze verwerking een vergunning aan te vragen.

Identificatiefase - Deze slimme technologie of slimme camera's zouden ook de functionaliteit kunnen hebben dat tijdens een wedstrijd verkregen beelden kunnen worden vergeleken met bestaand beeldmateriaal van personen, op basis waarvan de op de verzamelde beelden zichtbare personen kunnen worden geïdentificeerd. Men spreekt dan van de inzet van gezichtsherkenningstechnologie. Daarbij is dan sprake van de verwerking van biometrische gegevens als bedoeld in artikel 4, aanhef en onder 14, AVG. De verwerking van biometrische gegevens betreft de verwerking van bijzondere persoonsgegevens als bedoeld in artikel 9 AVG. Dat is verboden, tenzij de betrokken verwerkingsverantwoordelijke (bijvoorbeeld de BVO) zich op een doorbrekingsgrond kan beroepen. Vooralsnog zien wij niet een dergelijke doorbrekingsgrond. Om deze reden concluderen wij dat de inzet van deze slimme technologie **–** de zgn. gezichtsherkenningstechnologie **–** in de identificatiefase niet toelaatbaar is. Ook de inzet van andere slimme technologie die werkt met biometrische gegevens, zoals stemherkenningstechnologie, achten wij niet toelaatbaar vanwege het ontbreken van een doorbrekingsgrondslag.

Sanctiefase - Het uiteindelijke doel van het in de signalerings- en identificatiefase verkregen materiaal is dat er een sanctie kan worden opgelegd aan degenen die zich schuldig hebben gemaakt aan discriminatoir of racistisch gedrag. Wij concluderen in dit rapport dat de in de signaleringsfase verkregen opnames kunnen worden doorgegeven aan de desbetreffende instanties voor zover dat noodzakelijk is voor civielrechtelijke en/of strafrechtelijke handhaving. Voor verstrekking van biometrische gegevens zien wij geen ruimte, omdat voor het aanvankelijk verzamelen van die gegevens al geen grondslag bestaat. We zien daarentegen wel enige ruimte voor de daarbij betrokken partijen (waaronder de voetbalclub en de KNVB) om in het kader van de (rechts)procedure analyses in te zetten (zoals gezichts- of stemherkenningstechnologie) om de bewijswaarde van de beelden of geluidsopnamen te verhogen en daarbij bijzondere persoonsgegevens te verwerken, mits kan worden aangetoond dat de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering. De betreffende instanties moeten daarvoor zelf beschikken over referentiemateriaal.

Eindconclusie - De conclusie dat wij geen ruimte zien voor de inzet van gezichtsherkenningstechnologie in voetbalstadions, laat onverlet dat wij wel ruimte zien voor de inzet van slimme camera's. Daarmee kan discriminatoir en racistisch gedrag mogelijk in ieder geval beter worden gesignaleerd en vastgelegd. Bovendien kunnen de opnames die worden vastgelegd met slimme camera's het identificatieproces mogelijk vergemakkelijken, doordat de opnames gerichter zijn en van betere kwaliteit zijn. Voor zover de inzet van slimme camera's in de signaleringsfase tot onvoldoende verbetering leidt van de identificatiemogelijkheden in de identificatiefase, en daardoor ook tot onvoldoende verbetering van de sanctiemogelijkheden, kan worden overwogen om met een vorm van preregistratie te gaan werken om identificatiemogelijkheden van betrokkenen te verbeteren.

2.2 De keuzeladder

De hierboven weergegeven conclusie betreft een gesimplificeerde weergave van onze bevindingen. In iedere fase zijn verschillende middelen denkbaar om tot signalering, identificatie respectievelijk sanctieoplegging te komen.

Om de verwerkingsverantwoordelijken te helpen bij de onderbouwing van hun keuze om al dan niet over te gaan tot de inzet van slimme technologie, hebben wij in dit rapport een zgn. keuzeladder opgenomen per fase. Deze ladder begint bij het minst ingrijpende middel dat kan worden ingezet voor signalering, identificatie of sanctieoplegging, en eindigt bij het meest ingrijpende middel.

Daarbij hebben wij per middel aanbevelingen gedaan voor de technische maatregelen die kunnen worden getroffen om te waarborgen dat alleen de strikt noodzakelijke persoonsgegevens worden verwerkt en het vereiste van privacy by design & default in acht wordt genomen. Dat doen wij aan de hand van een zgn. stoplichtmodel:

- Groen houdt in dat het desbetreffende middel in overeenstemming met de AVG kan worden ingezet, zonder dat de verwerkingsverantwoordelijke wezenlijke technische en/of organisatorische maatregelen hoeft te treffen;
- Oranje duidt erop dat (i) het middel alleen kan worden ingezet voor zover de verwerkingsverantwoordelijke aantoont dat de eerdergenoemde, minder ingrijpende middelen niet effectief genoeg waren en (ii) organisatorische of technische maatregelen worden getroffen om het gebruik van het middel/de technologie in overeenstemming te brengen met de AVG. Wij kleuren deze optie dan oranje, omdat deze optie in lijn gebracht *kan* worden met de AVG, mits (de strikte noodzaak van) die keuze zorgvuldig kan worden onderbouwd en de nodige privacywaarborgende maatregelen worden getroffen;
- Rood duidt erop dat de slimme technologie niet in lijn is met de AVG, omdat er (op dit moment) geen toereikende wettelijke grondslag en/of strikte noodzaak bestaat.

Hieronder treft u per fase de keuzeladder aan met de belangrijkste bevindingen die daaraan ten grondslag liggen.

2.2.1 Fase 1 – Signaleren van discriminatie en racisme

Een slimme technologie die kan worden ingezet ten behoeve van de signalering van discriminatie en racisme betreft de inzet van slimme camera's en microfoons, al dan niet gecombineerd met emotieherkenningstechnologie.

Binnen de huidige gegevensbeschermingswetgeving – de (U)AVG – zien wij ruimte om slimme camera's en microfoons in te zetten ten behoeve van de signalering van discriminatie en racisme (en, in het verlengde daarvan, voor de identificering en sanctieoplegging). De grondslag hiervoor kan worden gevonden in het

gerechtvaardigde belang van de BVO's, de KNVB en/of van de personen tot wie discriminatie of racisme zich richt, en natuurlijk ook het maatschappelijk belang bij het tegengaan van rascisme en discriminatie (artikel 6, eerste lid, aanhef en onder f, AVG).

Een belangrijke voorwaarde is dat de verwerkingsverantwoordelijke (zoals de BVO) zorgvuldig en gedegen onderbouwt dat de inzet van (een combinatie van) slimme technologie (in aanvulling op reeds bestaande middelen) strikt noodzakelijk is voor de daarmee beoogde doeleinden. Dit houdt concreet in dat de meerwaarde en effectiviteit zorgvuldig moet worden aangetoond aan de hand van objectieve feiten. In aanvulling daarop dient de verwerkingsverantwoordelijke te onderbouwen dat de belangen van de BVO, van de KNVB en van de voetbalspelers of supporters die het mikpunt zijn van racisme of discriminatie zwaarder wegen dan het privacybelang van de betrokken toeschouwers. Aandachtspunt is daarbij dat de gevolgen van de inzet van de slimme technologie − uiteraard afhankelijk van het ontwerp en de aard van de technologie − vergaand kunnen zijn. Het is tegen deze achtergrond van belang dat de verwerkingsverantwoordelijken aanvullende waarborgen per technologie treffen om onevenredige gevolgen voor de betrokkenen te voorkomen.

Voor de inzet van emotieherkenningstechnologie bestaat onzes inziens geen grondslag nu de noodzaak om deze technologie in te zetten ten behoeve van de signalering en aanpak van discriminatie en racisme niet aanwezig lijkt te zijn. Daarvoor achten wij met name van belang dat de inzet van emotieherkenningstechnologie niet of beperkt lijkt bij te dragen aan het kunnen aanpakken van discriminatoir of racistisch gedrag.

Bijzondere persoonsgegevens

Op voorhand lijkt ervan uit te kunnen worden gegaan dat de met de inzet van slimme camera's en microfoons in fase 1 geen bijzondere persoonsgegevens worden verwerkt. De AP legt op haar website uit dat zij beeldmateriaal niet aanmerkt als bijzondere persoonsgegevens indien:[3]

1. het verkrijgen van dat beeldmateriaal niet is gericht op ras, etniciteit, religie of gezondheid;
2. het niet te voorzien is dat er op basis van het beeldmateriaal onderscheid gaat worden gemaakt naar ras, etniciteit, religie of gezondheid; en
3. onvermijdelijk is dat dergelijke gegevens worden verwerkt bij het maken van het beeldmateriaal.

Pas als het maken van beeldopnames is gericht op bijzondere persoonsgegevens en/of op basis van de opnames onderscheid zal worden gemaakt naar ras, etniciteit, religie of gezondheid, moet ervan uit worden gegaan dat de beelden kwalificeren als

[3] Zie www.autoriteitpersoonsgegevens.nl > onderwerpen > foto en film > beeldmateriaal. Zie ook EDPB, Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur, versie 2.0, vastgesteld op 29 januari 2020, nr. 62 e.v.; alsmede de in paragraaf 4.2.1 (in de voetnoten) aangehaalde beleidstukken. Zie ook conclusie A-G Machielse, 16 mei 2017, ECLI:NL:PHR:2017:547.

bijzondere persoonsgegevens. De AP neemt in haar beleidsregels tot uitgangspunt dat indien de verwerking van (bijzondere persoonsgegevens op) camerabeelden *identificatie* tot doel heeft, deze beelden als een rasgegeven moeten worden aangemerkt.[4] Dat is volgens de AP niet het geval bij bijvoorbeeld camera's die worden opgehangen in winkels om personen en/of goederen te beveiligen. Het voorgaande maakt dat in de identificatiefase mogelijk wél bijzondere persoonsgegevens worden verwerkt (zie paragraaf 2.2.2 van dit rapport). Wij merken op dat de inzet van slimme camera's met emotieherkenning naar verwachting niet leidt tot de verwerking van bijzondere persoonsgegevens.

Strafrechtelijke persoonsgegevens

Het valt niet uit te sluiten dat met de inzet van slimme technologie strafrechtelijke persoonsgegevens worden verwerkt. Daarvan is − kort gezegd - sprake als uit de beelden zodanige concrete feiten en omstandigheden blijken dat zij een bewezenverklaring van een strafbaar feit kunnen dragen, waarbij als maatstaf dient te worden genomen dat de vastgestelde gedragingen een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren.[5] Het strafbare discriminerend of racistisch gedrag dient in voldoende mate vast te staan. Aangezien de inzet van slimme technologie specifiek tot doel heeft om dergelijk gedrag te signaleren en identificeren, zullen voetbalclubs (of andere verwerkingsverantwoordelijken) niet kunnen uitsluiten dat bij de inzet van slimme technologie beelden worden vastgelegd die een dergelijke (strafrechtelijke) verdenking kunnen dragen. Aangezien in zoverre niet kan worden uitgesloten dat strafrechtelijke persoonsgegevens worden verwerkt, dient de voetbalclub te beschikken over een expliciete grondslag voor de verwerking van strafrechtelijke persoonsgegevens als bedoeld in artikel 10 AVG, respectievelijk de artikelen 31 − 33 UAVG.

De meest realistische grondslag voor de verwerking van strafrechtelijke persoonsgegevens betreft artikel 33, vierde lid, aanhef en onder c, AVG dat bepaalt dat een dergelijke verwerking is toegestaan indien de AP daarvoor een vergunning heeft verleend. Een dergelijke vergunning zou gezamenlijk door de BVO's kunnen worden ingediend.

Voor de specifieke situaties waarin het gaat om de verwerking van beelden van racistische of discriminerende uitingen die zijn gericht tegen de eigen werknemers van de voetbalclub, zou ook artikel 33, tweede lid, aanhef en onder b, UAVG uitkomst kunnen bieden. In artikel 33, tweede lid, aanhef en onder b, UAVG is bepaald dat een verwerkingsverantwoordelijke strafrechtelijke persoonsgegevens mag verwerken ter bescherming van zichzelf met betrekking tot (gepleegde of te plegen) strafbare feiten jegens hem of zijn werknemers.

---

4 AP, 'Cameratoezicht. Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens', 2 februari 2016, p. 26.

5 Zie o.a. Rb. Den Haag 12 januari 2017, ECLI:NL:RBDHA:2017:264, rov. 4.12-14; Rb. Midden-Nederland 20 februari 2017, ECLI:NL:RBMNE:2017:805, rov. 4.8 en Rb. Amsterdam 22 maart 2018, ECLI:NL:RBAMS:2018:3354 en ECLI:NL:RBAMS:2018:3355, rov. 4.5.

Wij achten laatstgenoemde grondslag echter minder goed bruikbaar dan het aanvragen van een vergunning bij de AP, aangezien deze bepaling slechts de verwerkingen ten eigen behoeve van de voetbalclub rechtvaardigden. (Onder andere) de verstrekking van beelden (die gezien de aard van de beelden kwalificeren als strafrechtelijke persoonsgegevens) aan anderen (waaronder de KNVB of de politie) kan niet op deze grondslagen worden gebaseerd. Daarbij geldt bovendien dat de BVO deze grondslag enkel kan inroepen ter bescherming van zichzelf of zijn eigen werknemers. Ook in zoverre is de bruikbaarheid van deze doorbrekingsgrondslag beperkt.

Keuzeladder

De keuzeladder voor de toepassing van slimme technologieën in de signaleringsfase ziet er als volgt uit.

Relatief lage privacyinbreuk Relatief hoge privacyinbreuk

(a)	Signalering door scheidsrechters, grensrechters officials en stewards	
Beoordeling De minst inbreukmakende maatregel die kan worden ingezet is het door de scheidsrechter, grensrechter, officials of stewards real-time constateren van racistische en discriminerende uitingen.		
Aanbevelingen privacy by design & default Geen specifieke aanbevelingen.		

(b)	Gebruik en verbetering van reeds bestaande videosystemen (zonder slimme technologie)	
Beoordeling Op dit moment zetten BVO's reeds video-installaties in voor het vaststellen van ongeregeldheden die plaatsvinden binnen de toeschouwersvakken. Dat is verplicht op grond van de licentie-eisen van de KNVB. Voordat wordt overgegaan tot de inzet van slimme(re) camera's en microfoons, is allereerst van belang dat BVO's nagaan of verbetering van de kwaliteit van deze video-installaties al tot de gewenste verbetering van signaleringsmogelijkheden kan leiden.		
Aanbevelingen privacy by design & default • Stel de camera's zo in dat in beginsel ieder vak wordt gefilmd, maar borg dat enkel de relevante beelden worden geselecteerd voor nader onderzoek. • Bewaar de verkregen beelden en de persoonsgegevens voor een beperkte, strikt noodzakelijke termijn. • Beperk de omvang van de personen die toegang hebben tot beelden tot het strikt noodzakelijke. Een en ander dient te worden uitgewerkt in een concreet autorisatiebeleid. Werk in dit beleid waar mogelijk uit wanneer nader		

onderzoek ten behoeve van de signalering van discriminatie of racisme mag worden overgegaan.

- Overweeg een evaluatieprotocol op te stellen, waarmee de BVO doorlopend kan bezien of het gebruik van de bestaande videosystemen voldoende effectief zijn. Voor zover zich signalen voordoen dat de effectiviteit of de bewijswaarde van de bestaande videosystemen te wensen overlaat, kunnen deze evaluaties als grondslag dienen voor de keuze van meer ingrijpende slimme technologieën.

(c)	**Inzet slimme camera's en microfoons**	

(a) *Beoordeling*

Onze inschatting is dat slimme camera's en microfoons een noodzakelijke en proportionele maatregel kan vormen voor het bestrijden van discriminatie en racisme. Van belang daarbij is dat de slimme camera's en de slimme geluidsdetectie zo wordt ingesteld en getraind dat deze zoveel mogelijk alleen de relevante beelden en geluiden opvangen. Dit houdt onder meer in dat beelden en geluiden die niet relevant zijn niet worden opgenomen, dan wel gepseudonimiseerd worden bewaard en zo snel mogelijk worden verwijderd. Het zijn specifiek dergelijke instellingen die in het concrete geval zullen bepalen of de gekozen slimme technologie daadwerkelijk proportioneel kan worden geacht.

Aanbevelingen privacy by design & default

(b)

- Stel waar mogelijk de slimme camera's en microfoons zo in dat minder opnames worden gemaakt in vergelijking tot de achter (b) genoemde camerabeelden, bijvoorbeeld door de apparatuur zo in te stellen dat zij pas gaat opnemen en opslaan zodra racisme en discriminatie wordt gedetecteerd. Voor zover het niet mogelijk of wenselijk is dat de camera's pas bij een specifiek incident van start gaan met het daadwerkelijk registreren van de beelden of geluiden, zou de BVO het vaste beleid moeten hanteren dat de beelden versleuteld worden opgeslagen en slechts de door de slimme technologie geselecteerde beelden met het mogelijke onrechtmatige gedrag worden getoond aan de desbetreffende medewerker. Dit met het oog op het dataminimalisatie-beginsel.

- Gebruik slechts slimme technologieën waarvan de effectiviteit in voldoende mate op basis van (wetenschappelijk) onderzoek is vastgesteld, en waarvan informatie beschikbaar is over de validatie van het achterliggende algoritme en over de verificatie van de aan het algoritme ten grondslag liggende factoren. Uit deze informatie moet in ieder geval blijken welke stappen zijn genomen in de ontwikkeling en validatie van de indicatoren van de technologieën (en of, en zo ja, door wie deze zijn gepeer-reviewed), alsook welke statistische trainingsmodellen gebruikt zijn.

- Licht in een verantwoordingsdocument (waar mogelijk) toe hoe de selectie van de beelden en het geluid plaatsvindt en motiveer daarbij standaard wat de daarvoor onderliggende variabelen zijn.

- Overweeg ook hier een evaluatieprotocol op te stellen, waarmee de BVO doorlopend kan bezien of het gebruik van de slimme technologie voldoende effectief is. Voor zover zich signalen voordoen dat de effectiviteit of de bewijswaarde van de bestaande videosystemen te wensen overlaat, kunnen deze evaluaties als grondslag dienen voor de keuze van meer ingrijpende slimme technologieën.

- Zorg ervoor dat periodiek ook handmatig tijdens een wedstrijd mogelijke discriminerende uitlatingen worden geselecteerd. Op deze manier kan worden gecontroleerd of de slimme technologieën juist staan afgesteld. Eventuele

discrepanties zouden een aanleiding kunnen zijn om te onderzoeken of de slimme technologie niet naar behoren functioneert of niet juist is afgesteld.

(d)	**Slimme camera's met emotieherkenning**	
Beoordeling De in onze optiek meest privacygevoelige soort slimme camera's betreft camera's met emotieherkenning. Wij betwijfelen de noodzaak van de inzet van emotieherkenning. Eerst zou moeten worden aangetoond dat controle van de (door slimme technologie geselecteerde) beelden en geluid niet handmatig of door middel van de achter (c) genoemde middelen kunnen worden geanalyseerd. Onze twijfel aan de noodzaak is mede ingegeven door de omstandigheid dat emotieherkenning – gezien de huidige stand van de techniek en gezien de vaststelling dat discriminatie niet altijd gekoppeld is aan een specifieke emotie – slechts een beperkte aanvullende meerwaarde zal hebben ten opzichte van de achter (c) genoemde slimme technieken. Dat is ook in de marktverkenning onderkend.		
Aanbevelingen privacy by design & default Geen aanbevelingen.		

2.2.2 Fase 2 – Identificeren van de betrokkene

De slimme technologie die kan worden ingezet ten behoeve van de identificatie van de betrokkene betreft de inzet van gezichtsherkenningstechnologie en eventueel ook stemherkenningstechnologie.

Binnen de huidige gegevensbeschermingswetgeving – de (U)AVG – zien wij geen ruimte om gezichtsherkenningssoftware in te zetten dan wel anderszins biometrische gegevens te verwerken met het oog op de unieke identificatie van een persoon. Op dit moment lijkt er geen uitzonderingsgrond te bestaan in de (U)AVG waarop BVO's of de KNVB zich kunnen beroepen om het verbod op de verwerking van biometrische gegevens te doorbreken.

Een andere optie is het werken met stoelnummerregistratie. Van toeschouwers wordt dan verlangd dat zij zich bij de aanschaf van een toegangsbewijs met hun persoonsgegevens (en eventueel ook met foto) registreren (zgn. preregistratie), en zij vervolgens bij hun toegangsbewijs een stoelnummer krijgen toegewezen. Door localisatiesoftware kan worden achterhaald op welk stoelnummer een incident plaatsvond en welke toeschouwer op dat stoelnummer staat geregistreerd. Met behulp van deze informatie in combinatie met de beeld- en geluidsopnames van een incident kan de betrokkene dan (deels handmatig) worden geïdentificeerd.

Voor identificatie door middel van stoelnummerregistratie (preregistratie en locatiesoftware die herleidbaar is tot stoelnummers) zien wij wel ruimte. De grondslag daarvoor kan worden gevonden in het gerechtvaardigd belang (artikel 6, eerste lid, aanhef en onder f, AVG). Daarbij zal de verwerkingsverantwoordelijke de noodzaak van de preregistratie in combinatie met de locatiesoftware moeten onderbouwen en voldoende maatregelen moeten treffen om de omvang en aard van de verwerking te beperken tot het strikt noodzakelijke.

Wij kunnen ons voorstellen dat deze optie reeds een significante verbetering meebrengt van de identificatiemogelijkheden ten opzichte van de huidige situatie. Daarbij speelt ook een rol dat door de inzet van slimme camera's en microfoons in de signaleringsfase de kwaliteit van het beeld- en geluidmateriaal dusdanig kan verbeteren dat daarmee ook de (gedeeltelijk) handmatige identificatie in combinatie met stoelnummerregistratie na een incident wordt vergemakkelijkt.

Bijzondere persoonsgegevens

Hoewel in de identificatiefase de inzet van gezichtsherkenningstechnologie zou kunnen bijdragen aan de vaststelling van de identiteit van de potentiële dader (en daarmee aan de bewijsvoering in de sanctiefase), lijkt een toereikende doorbrekingsgrond voor de biometrische gegevens die daarbij worden verwerkt, te ontbreken. Wij zien daarom geen mogelijkheden om in de identificatiefase gezichtsherkenningstechnologie in te zetten, nog daargelaten dat dergelijke gezichtsherkenning enkel kan worden ingezet

voor zover de BVO reeds eerder referentiemateriaal (zoals een foto bij de toegangspoort) heeft verwerkt.

Wij merken hier ook op dat de identificatie van personen door middel van (stoelnummerregistratie in combinatie met) beelden, waaruit ook informatie is af te leiden over iemands religie, gezondheid, ras of etniciteit, niet reeds hoeft te maken dat daarmee bijzondere persoonsgegevens worden verwerkt. De verwerking van beelden betreft pas een verwerking van bijzondere persoonsgegevens, op het moment dat de (indirecte) bijzondere persoonsgegevens worden geanalyseerd met als doel het (op basis van dat gegeven) identificeren van de desbetreffende persoon. Voor zover daarover discussie zou ontstaan, is er een doorbrekingsgrond aanwezig voor de onvermijdelijke verwerking van eventuele (indirecte) ras of etniciteitsbeelden die zichtbaar zijn op de beelden of uit geluidsfragmenten blijken. De verwerking van dergelijke beelden met persoonsgegevens over iemands ras of etniciteit is op grond van de UAVG namelijk toegestaan indien de analyse plaatsvindt met het oog op de identificatie van de desbetreffende persoon, en slechts voor zover de verwerking voor dat doel onvermijdelijk is (artikel 25, aanhef en onder a, UAVG).

Keuzeladder

De keuzeladder voor de toepassing van slimme technologieën in de identificatiefase ziet er als volgt uit.

Relatief lage privacyinbreuk — Relatief hoge privacyinbreuk

(a)	Handmatige identificatie van personen	
(c) *Beoordeling* De minst ingrijpende maatregel is de handmatige analyse van de (eventueel met slimme technologie in fase 1) verkregen beelden en, aan de hand daarvan, de handmatige identificatie van personen. Hoewel (relatief) privacyvriendelijk, is voor de handmatige identificatie in veel gevallen veel mankracht vereist. Het is bovendien voor de voetbalclubs in veel gevallen moeilijk om personen buiten de vaste supporterskern te kunnen identificeren. Deze vaststelling kan in onze optiek rechtvaardigen dat zwaardere middelen worden ingezet om identificatie van personen mogelijk te maken, bijvoorbeeld door de preregistratie te verbeteren.		
Aanbevelingen privacy by design & default Geen specifieke aanbevelingen.		

(b)	Handmatige identificatie van personen met preregistratie	

Beoordeling

Een relatief zwaarder middel zou zijn dat de voetbalclubs ervoor kiezen om de preregistratie te verbeteren, zodat op basis van de beelden van het vastgelegde incident het stoelnummer kan worden gekoppeld aan de persoonsgegevens die vooraf zijn geregistreerd voor dat stoelnummer. Bij deze werkwijze wordt geen gebruik gemaakt van preregistratie met een foto.

Aanbevelingen privacy by design & default

- Zorg dat de preregistratie-bestanden geautomatiseerd worden verwijderd op het moment dat geen nader onderzoek meer noodzakelijk is.

(c)	Handmatige identificatie van personen met preregistratie inclusief foto	

Beoordeling

Indien kan worden onderbouwd dat het gebruik van een foto de effectiviteit en de betrouwbaarheid van de identificatie aanzienlijk vergroot, kan in onze optiek worden gekozen voor het maken van beelden van personen bij de ingang van de voetbalstadions.

Aanbevelingen privacy by design & default

- Om de inbreuk op de privacy van betrokkenen te beperken tot het strikt noodzakelijke zouden de gegevens die worden verzameld bij de preregistratie versleuteld kunnen worden opgeslagen, totdat op basis van de beelden aanleiding bestaat om nader onderzoek te verrichten naar personen op specifieke stoelnummers. De relevante stoelnummers (incl. de foto van de personen die bij de toegangspoort hun kaartjes hebben laten scannen) zouden vervolgens kunnen worden ontsloten ten behoeve van het onderzoek.

- Van belang is tot slot dat de versleutelde dataset (met daarin de bij de toegang gemaakte foto's gekoppeld aan het stoelnummer op het kaartje) geautomatiseerd wordt verwijderd op het moment dat geen nader onderzoek meer noodzakelijk is.

(d)	Biometrische identificatie	

Beoordeling

De meest privacygevoelige keuze zou de inzet van gezichts- en/of stemherkenningstechnologie zijn. In dat geval worden de opgenomen beelden (en eventueel ook geluiden) geautomatiseerd door middel van biometrische toepassingen geanalyseerd en worden betrokkenen op basis van die analyse geïdentificeerd. Op dit moment zien wij daar geen toereikende (doorbrekings)grondslag voor.
(d)

Aanbevelingen privacy by design & default

(e) Geen aanbevelingen

2.2.3 Fase 3 – Gebruik van de gegevens ten behoeve van sanctieoplegging

De door middel van de inzet van slimme technologie verkregen bewijsmiddelen kunnen vervolgens worden ingezet ten behoeve van het opleggen van sancties. Het slachtoffer, de voetbalclub, de KNVB en het OM beschikken over de volgende mogelijkheden om een sanctie op te (laten) leggen voor discriminatoire of racistische gedragingen.

Zie bijlage 2 bij dit rapport voor een uitvergrote versie van de sanctiekaart.

Verdere verwerking

Het verstrekken van de beelden en geluidsopnamen en de bijbehorende gegevens door de BVO aan een derde partij (bijvoorbeeld aan een andere voetbalclub, de KNVB of de politie, de deskundigen of de behandelaren/beoordelaars respectievelijk de rechters van de zaak) ten behoeve van het opleggen van een sanctie betreft een verdere verwerking. Wij menen dat deze verwerking verenigbaar is met het oorspronkelijke doeleinde van de verzameling. Het opleggen van een sanctie aan overtreders staat in een direct verband met het oorspronkelijke doel van de verzameling (het signaleren en identificeren van onrechtmatig gedrag en de zorgplicht om onrechtmatigheden binnen het stadion te voorkomen). Doordat sprake is van een verenigbare verdere verwerking hoeft de BVO niet te beschikken over een aparte wettelijke grondslag voor de verstrekking.

Ervan uitgaande dat de BVO (en/of eventuele andere verwerkingsverantwoordelijken) de noodzaak van de in identificatie- en signaleringsfase gekozen slimme technologieën goed heeft onderbouwd, kunnen de daarmee verkregen beeld- en geluidsopnames en andere (identificatie)gegevens evenzeer worden gebruikt voor het uiteindelijk opleggen van een sanctie aan de desbetreffende persoon. Van belang daarbij is overigens wel dat het bewijs beperkt blijft tot de strikt noodzakelijke, toereikende en relevante beelden, geluiden en persoonsgegevens. Andere gegevens zullen zo veel mogelijk moeten worden verwijderd.

Bijzondere & strafrechtelijke persoonsgegevens

Evenals in de identificatiefase menen wij dat in de sanctiefase niet zonder meer gebruik kan worden gemaakt van gezichts- en/of stemherkenningstechnologie, omdat een doorbrekingsgrond voor biometrische persoonsgegevens ontbreekt. De uitzonderingsgrond van artikel 29 UAVG (de verwerking van biometrische gegevens is noodzakelijk voor authenticatie of beveiliging) doet zich in deze fase niet voor, aangezien in de sanctiefase dergelijke beveiligingsdoeleinden niet worden nagestreefd.

Bijzondere persoonsgegevens die rechtmatig in de identificatiefase zijn verwerkt (bijvoorbeeld omdat de beelden rasgegevens bevatten die (onvermijdelijk) zijn verwerkt voor de identificatie van de persoon)[6] mogen, evenals strafrechtelijke persoonsgegevens, verder worden verwerkt als bewijs ten behoeve van een civiele of strafrechtelijke procedure tegen de dader, mits er daadwerkelijk één van de in de sanctiekaart genoemde (rechts)middelen is ingezet en de verwerking van deze gegevens strikt noodzakelijk zijn voor de instelling, uitoefening of onderbouwing van een rechtsvordering (zie artikel 22, tweede lid, aanhef en onder e, UAVG jo. artikel 32, aanhef en onder d, UAVG). Deze noodzaak kan worden aangenomen als de beelden strikt noodzakelijk zijn voor de bewijsvoering.

[6] Artikel 25, aanhef en onder a, UAVG.

Wij benadrukken dat de bewijsmiddelen (met daarin bijzondere of strafrechtelijke persoonsgegevens) ook in het kader van de aangifte aan de politie mogen worden verstrekt. Hoewel dit niet expliciet wordt opgemerkt in de aangiftebevoegdheid van artikel 161 Sv, is goed verdedigbaar dat bij een aangifte strafrechtelijke gegevens kunnen worden verstrekt. Een aangifte heeft immers per definitie betrekking op een (vermeend) strafbaar feit. In zoverre is artikel 161 Sv een lidstatelijke bepaling als bedoeld in artikel 10 AVG. De verwerking van bijzondere persoonsgegevens in de aangifte kan vervolgens worden gebaseerd op artikel 23, aanhef en onder c, UAVG dat bepaalt dat bijzondere persoonsgegevens (voor zover noodzakelijk) in aanvulling op strafrechtelijke persoonsgegevens mogen worden verwerkt.

Voor zover de aanpak in fase 3 een civielrechtelijke procedure betreft (bijvoorbeeld een procedure ten behoeve van het opleggen van een stadionverbod door de KNVB) zien wij gedurende deze procedure een potentiële doorbrekingsgrond voor de verwerking van biometrische gegevens met het oog op het opleggen van een sanctie aan betrokkenen. Het gaat hier om het de situatie dat een door de voetbalclub, KNVB of rechter aangestelde deskundige door middel van een analyse de bewijswaarde van de beelden of geluidsfragmenten poogt te verbeteren ten behoeve van een regionale of landelijke procedure die door de BVO of de KNVB is ingesteld voor het opleggen van (niet-strafrechtelijke) sancties, waaronder het opleggen van het stadionverbod. Het doel daarvan is het verhogen van de bewijswaarde van de vaststelling van het delict of de identificatie van de dader aan de hand van de biometrische analyse van beelden en geluidsopnamen of andersoortige analyses waarbij bijzondere persoonsgegevens worden gemaakt (bijvoorbeeld het toepassen van stem- of gezichtsanalyses e.d.). Wij menen dat voor deze concrete situatie naar verwachting wél een doorbrekingsgrond als bedoeld in artikel 9, tweede lid, AVG zou kunnen bestaan voor de verwerking van bijzondere gegevens, mits kan worden aangetoond dat het strikt noodzakelijk is dat de deskundige een geautomatiseerde (biometrische) analyse verricht. Een dergelijk verwerking zou gebaseerd kunnen worden op artikel 22, aanhef en onder e, UAVG dat bepaalt dat bijzondere persoonsgegevens mogen worden verwerkt voor zover dat noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Voor zover de deskundige een beroep wil doen op bovenstaande uitzonderingsgrond voor de inzet van biometrie, wijzen wij op de volgende aandachtspunten om de strikte noodzaak en de privacy by design en default te borgen:

- Gebruik slechts slimme (biometrische) technologieën waarvoor in voldoende mate wetenschappelijk onderzoek bestaat over de effectiviteit van de technologie, evenals informatie over de validatie van het achterliggende algoritme en verificatie van de aan het algoritme ten grondslag liggende factoren. Uit deze informatie moet in ieder geval blijken welke stappen genomen zijn in de ontwikkeling en validatie van de indicatoren van de technologieën, alsook welke statistische trainingsmodellen gebruikt zijn.

- Licht in een verantwoordingsdocument (waar mogelijk) toe hoe de analyse van de beelden en het geluid plaatsvindt en motiveer daarbij standaard wat daarvan de onderliggende variabelen zijn.

- Overweeg ook hier een evaluatieprotocol op te stellen, waarmee de BVO of de deskundige doorlopend kan bezien of het gebruik van de slimme technologie voldoende effectief is. Voor zover zich signalen voordoen dat de effectiviteit of de bewijswaarde van de bestaande videosystemen te wensen overlaat, kunnen deze evaluaties als grondslag dienen voor de keuze van meer ingrijpende slimme technologieën.

- Zorg ervoor dat − naast het enkele gebruik van de slimme technologieën − ook altijd steekproefsgewijs gedurende een wedstrijd handmatig mogelijke discriminerende uitlatingen worden geselecteerd. Op deze manier kan worden gecontroleerd of de slimme technologieën juist staan afgesteld. Bij eventuele discrepanties zou dit een aanleiding kunnen zijn dat de slimme technologie niet naar behoren functioneert of niet juist is afgesteld.

2.3 Tot slot

Los van het voorgaande moet iedere verwerking van persoonsgegevens met slimme technologie (ook) voldoen aan de overige voorwaarden uit de (U)AVG, en moeten de rechten van de betrokkenen in acht worden genomen. Wij lichten dit in hoofdstuk 8 en 9 nader toe. Wij komen tot de volgende aanbevelingen.

§ 8.2	Geef niet zomaar persoonsgegevens door naar derde landen

Toelichting

Indien persoonsgegevens worden verwerkt buiten de Europese Unie, is sprake van de internationale doorgifte van persoonsgegevens. Een dergelijke situatie doet zich bijvoorbeeld voor indien de BVO in het kader van de inzet van de slimme technologie of de opslag van de beelden gebruik zou maken van een Amerikaanse cloudopslagprovider die op buitenlandse servers ten behoeve van de BVO persoonsgegevens verwerkt. Een ander voorbeeld is dat de BVO de beelden en geluidsopnamen verstrekt aan een voetbalclub buiten de EU.

Aanbevelingen

- Gezien de gevoeligheid van de beelden en geluidsopnamen, raden wij aan om waar mogelijk internationale doorgifte aan derde landen te voorkomen. Dat geldt in het bijzonder bij het implementeren van cloudoplossingen.

- In het geval van doorgifte van persoonsgegevens aan derde landen, zal hetzelfde hoge beveiligingsniveau als in de AVG moeten worden gegarandeerd.

- Een bijzonder aandachtspunt in dit kader is nog dat het Europese Hof van Justitie ('HvJ') bij uitspraak van 16 juli 2010 in de zaak C-311/18 (Schrems II) het zogenoemde 'Privacy Shield' ongeldig verklaart. Dit betekent dat de doorgifte van persoonsgegevens aan Amerikaanse verwerkers niet langer gebaseerd kan worden op dit adequaatheidsbesluit.

§ 8.3	Persoonsgegevens worden verwerkt op een ten aanzien van de betrokkene rechtmatige, behoorlijke en transparante wijze.

Toelichting

Er bestaat een risico dat bij de inzet van slimme technologieën – met name de slimme technologieën waarbij beelden en opnamen geautomatiseerd worden gemaakt en/of geanalyseerd door een algoritme – onbedoeld verboden onderscheid wordt gemaakt op leeftijd, geslacht of ras/etniciteit. Zonder strikte waarborgen in zowel het ontwikkelproces als de toepassing van de technologie, kan dergelijke discriminatie onbedoeld tot vertekende resultaten leiden.

Los van de verwerkingsverantwoordelijkheid van de partij die de slimme technologie inzet, vervult de ontwikkelaar van de aan de slimme technologie ten grondslag liggende algoritmes een sleutelrol bij het voorkomen van onbedoeld verboden onderscheid.

Aanbevelingen

- Stel voorafgaand aan de ontwikkeling van het algoritme een strategie of een protocol vast om te voorkomen dat ongerechtvaardigde vertekening wordt gecreëerd of versterkt. Daarbij dient oog te zijn voor zowel de inputgegevens als het ontwerp van het algoritme.

- Zorg voor een klachtmechanisme waardoor het voor betrokkenen en derden mogelijk wordt om vertekening, discriminatie of slechte prestaties van het algoritme te melden. Zorg in aanvulling daarop voor een protocol waarin wordt beschreven op welke wijze dergelijke klachten in behandeling zullen worden genomen. Neem een verwijzing naar dit protocol op in de onderlinge regeling wanneer er sprake is van gezamenlijke verwerkingsverantwoordelijkheid ten aanzien van (het algoritme behorende bij) de betreffende slimme technologie. Dit klachtenmechanisme is erop gericht om de juistheid, behoorlijkheid en rechtmatigheid van de inzet van de aan de slimme technologie ten grondslag liggende algoritme te borgen.

- Laat voorafgaand aan de toepassing van het algoritme en de slimme technologie een onafhankelijke audit verrichten naar de mogelijke bias en discriminatoire effecten van het algoritme (zogenoemde 'discrimination testing'), bijvoorbeeld door de software en de code van het algoritme te laten toetsen door een technisch specialist.

- Test en monitor potentiële vertekeningen gedurende de toepassingsfase.
- Creëer bewustzijn bij de medewerkers van BVO'S en/of andere verwerkingsverantwoordelijken die de slimme technologie ontwikkelen of toepassen over de wijze waarop een bias kan ontstaan, welke gevolgen dit heeft en hoe dergelijke bias kan worden voorkomen.

§ 8.4	Persoonsgegevens dienen juist te zijn en zo nodig geactualiseerd te worden.

Toelichting

In artikel 5, eerste lid, aanhef en onder d, AVG is het beginsel van juistheid van de gegevens geformuleerd. Verwerkingsverantwoordelijken moeten op grond van artikel 5, eerste lid, aanhef en onder d, AVG alle redelijke maatregelen nemen om persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

Aanbevelingen

- Bouw altijd een menselijk controlemoment in waarbij wordt gecontroleerd of de koppeling van de beelden en de geluidsopnamen en de vaststelling van de identiteit van de betrokkene juist heeft plaatsgevonden.
- Geef een indicatie van de mate van (on)zekerheid van de kwaliteit en juistheid van de gemaakte beeld- en geluidsopnamen.[7] Licht bovendien toe wat de mate van (on)zekerheid bepaalt.
- Ontwerp een 'terugmeld-mechanisme', zodat eventuele in de ontwikkeling of toepassing van het algoritme en de slimme technologie vastgestelde onjuistheden of gebreken kunnen worden hersteld.
- Stel een periodiek controleproces vast dat (i) borgt dat fouten of vooroordelen in de verzamelde of gedeelde gegevens en (ii) fouten of vooroordelen in het algoritme worden opgemerkt. Stel daarbij concreet vast welke persoon of welke partij(en) dit controleproces uitvoert.
- Voer steekproefsgewijs een controle uit om te beoordelen of de aan de slimme technologieën ten grondslag liggende algoritmen voldoende nauwkeurig zijn. Voorkom daarmee overmatig vertrouwen in de uitkomsten van het algoritme en de slimme technologie. Daarbij kan gedacht worden aan een maatregel waarbij altijd naast de door het algoritme geselecteerde incidenten ook ter controle andere incidenten worden geselecteerd die het algoritme niet heeft geselecteerd. Indien blijkt dat deze incidenten wél hadden moeten worden geselecteerd, dan kan dit aanleiding vormen voor het bijstellen van het algoritme.
- Hanteer passende wiskundige en statistische procedures waarmee factoren die aanleiding geven tot onjuistheden van persoonsgegevens worden gecorrigeerd en het risico op fouten wordt geminimaliseerd.

§ 8.5	Bewaar persoonsgegevens niet langer dan noodzakelijk.

Toelichting

De BVO's, de KNVB en andere ontvangers van persoonsgegevens dienen strikte bewaartermijnen te formuleren voor de door slimme technologie vervaardigde beeld- en geluidsopnamen. Dat geldt ook voor andere persoonsgegevens die deze partijen verkrijgen, bijvoorbeeld in het kader van preregistratie.

Aanbevelingen

Geen specifieke aanbevelingen.

[7] Bijvoorbeeld: de voorspelling dat de gefilmde persoon ook degene is die de racistische leus heeft uitgesproken is voor 89% zeker.

§ 8.6	Zorg dat de persoonsgegevens passend beveiligd zijn.

Toelichting
De verwerkingsverantwoordelijke is verplicht om te waarborgen dat de persoonsgegevens die worden verwerkt als gevolg van de inzet van slimme technologie voldoende zijn beveiligd. Bovendien moet de verwerkingsverantwoordelijke erop toezien dat de getroffen beveiligingsmaatregelen ook daadwerkelijk worden nageleefd.

Aanbevelingen

- Stel een beveiligingsplan vast dat concreet is toegespitst op de toepassing van de slimme technologie en de daarmee geselecteerde beelden en geluidsopnamen, ga daarbij meer concreet in op de volgende aspecten:
- Toets periodiek de in het beveiligingsplan opgenomen maatregelen. Houd daarbij rekening met de stand van de techniek. Actualiseer voor zover nodig de beveiligingsmaatregelen.
- Waarborg – conform het hierboven genoemde beveiligingsplan – door middel van een autorisatiematrix en een controleproces dat degenen die toegang verkrijgen tot de omgeving van de slimme technologie, de geselecteerde geluidsopnamen en beelden en/of andere verkregen persoonsgegevens daadwerkelijk daartoe bevoegd zijn.
- Maak (met de gezamenlijke verwerkingsverantwoordelijken) heldere afspraken over het verrichten van audits en het geven van uitvoering aan de resultaten van beveiligingsaudits.
- Stel technische en organisatorische maatregelen vast (waaronder een noodplan) om eventuele schade te beperken in het geval een beveiligingsgebrek wordt geconstateerd.
- Waarborg dat eventuele (sub)verwerkers eveneens passende beveiligingsmaatregelen treffen.

§ 8.7	Verantwoord dat bij het gebruik van de technologie wordt voldaan aan de vereisten van de (U)AVG.

Toelichting
De verwerkingsverantwoordelijke voor (verwerking van persoonsgegevens met) de slimme technologie moet onder de AVG verantwoorden dat hij de beginselen en voorwaarden van de AVG naleeft. Dit volgt uit de in art. 5, tweede lid, AVG opgenomen 'verantwoordingsplicht'.

Aanbevelingen

- Stel een privacybeleid op waarin specifiek wordt ingegaan op de wijze waarop persoonsgegevens wordt verwerkt ten behoeve van de toepassing van de slimme technologie.
- Werk dit privacybeleid zo nodig uit in concrete privacy protocollen, zodat de medewerkers die de slimme technologie toepassen en/of de daarmee verkregen beeld- en geluidsopnamen en/of andere persoonsgegevens ontvangen op de hoogte zijn van de concrete stappen die zij moeten zetten om de privacy van betrokkenen te waarborgen.
- Neem in het verwerkingsregister een beschrijving op van de verwerkingen die plaatsvinden in het kader van de toepassing van de slimme technologie.

§ 8.8	Zorg dat datalekken tijdig gemeld worden.

Toelichting
De verwerkingsverantwoordelijken zullen bij eventuele datalekken[8] in specifieke gevallen verplicht zijn om deze te melden aan de AP en de betrokkenen.

[8] In de AVG wordt gesproken over een inbreuk in verband met persoonsgegevens. Dat is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (artikel 4 aanhef en onder 12 AVG). Er wordt gemakshalve gesproken van datalek.

Aanbevelingen
Geen specifieke aanbevelingen.

§ 8.9	Verricht voorafgaand aan de inzet van de technologie een DPIA.

Toelichting
Op grond van artikel 35 van de AVG moet de verwerkingsverantwoordelijke een data protection impact assessment ('DPIA') uitvoeren als een soort verwerking – in het bijzonder een waarbij nieuwe technologieën worden gebruikt – gelet op de aard en de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

De AP schrijft (onder meer) een DPIA voor bij cameratoezicht, profilering, observatie en de inzet van biometrie. Uit de door de AP geformuleerde criteria volgt dat voor de beoogde toepassingen van slimme technologieën een DPIA zal moeten worden verricht.

Aanbevelingen
Geen specifieke aanbevelingen.

§ 9.2	Informeer de betrokkene over de verwerkingen van persoonsgegevens.

Toelichting
De betrokkenen moeten overeenkomstig artikelen 13 en 14 AVG worden geïnformeerd over de verwerking van hun persoonsgegevens door middel van de inzet van (slimme) technologieën.

Het verdient aanbeveling om maatregelen te treffen die borgen dat de privacyverklaring (en eventuele wijzigingen in de inhoud daarvan) tijdig – en bij voorkeur geautomatiseerd – aan de betrokkene wordt verstrekt, bijvoorbeeld voorafgaand aan de aanschaf van een toegangskaart.

Voorts is van belang dat de BVO's en de KNVB, voor zover zij als gezamenlijke verwerkingsverantwoordelijken optreden, in een onderlinge regeling vaststellen hoe uitvoering wordt gegeven aan de informatieverplichting, en deze onderlinge regeling ter beschikking stellen aan betrokkenen.

Aanbevelingen

- Zorg ervoor dat, voorafgaand aan de inzet van slimme technologie waaraan een algoritme ten grondslag ligt, er altijd een externe audit is verricht van de technische werking en juistheid van het model (en een eventuele bias) en overweeg om deze uitkomsten op de website van de BVO of de KNVB beschikbaar te stellen (incl. de datum en uitslag van deze technische audit), tenzij zich daar reden toe verzetten. Archiveer de overwegingen waarom het beschikbaar stellen van de algemene toelichting op het algoritme niet wenselijk is.

- Overweeg om op de eigen website van de BVO of de KNVB een pagina in te richten waarop algemene informatie kan worden opgenomen over:
  - het doel van de slimme technologie
  - de wijze waarop de slimme technologie is ontwikkeld en toegepast.

- Stel een privacyverklaring op die voldoet aan de vereisten van art. 14 AVG, tenzij sprake is van een wettelijke uitzondering op de informatieverplichting.

- (Verplicht bij art. 14 AVG en voor zover sprake is van gezamenlijke verwerkingsverantwoordelijkheid) Maak heldere afspraken met de gezamenlijke verwerkingsverantwoordelijke(n) over de inhoud van de privacyverklaring, de wijze van het beschikbaar stellen daarvan en de procedure voor het wijzigen en actualiseren van de privacyverklaring. Neem deze afspraken vervolgens op in de onderlinge regeling die de gezamenlijke verwerkingsverantwoordelijken op grond van art. 26, eerste lid, AVG moeten opstellen. Het opstellen van een onderlinge regeling is onder de Wet justitiële en strafvorderlijke gegevens ('Wjsg') niet verplicht.

- Verstrek bij de toepassing van slimme technologie waarbij gebruik wordt gemaakt van een onderliggend algoritme nuttige informatie over de wijze van totstandkoming van het model, de validatie van het risicomodel en de verificatie van de risico-indicatoren. Deze informatie kan worden verstrekt op het moment dat de uitkomst met de betrokkene wordt gedeeld of na een bezwaar of verzoek om inzage van de betrokkene.

- Informeer de betrokkene over de methoden die door de BVO of de KNVB worden gebruikt om doorlopend te toetsen of de slimme technologie eerlijk, doelgericht en onbevooroordeeld blijft.

§ 9.3 tot en met § 9.9	Maak de uitoefening van de rechten van de betrokkene mogelijk.

Toelichting

Zorg dat bij de inzet van de technologie technische en organisatorische maatregelen zijn getroffen om de uitoefening van de in artikelen 15 tot en met 21 AVG genoemde rechten mogelijk te maken. Het gaat hier om:

- het recht op inzage (artikel 15 AVG);
- het recht op rectificatie (artikel 16 AVG);
- het recht op wissing (artikel 17 AVG);[9]
- het recht op beperking van de verwerking (artikel 18 AVG);
- het recht op dataportabiliteit (artikel 20 AVG); en tot slot
- het recht op bezwaar (artikel 21 AVG).

Aanbevelingen

Geen specifieke aanbevelingen.

[9] Het recht op wissing wordt ook wel aangeduid als het recht op vergetelheid.

DEEL 1

3 DE INZET VAN SLIMME TECHNOLOGIEËN: EEN INTRODUCTIE

Hieronder volgt een toelichting op de slimme technologieën die kunnen worden ingezet in stadions ten behoeve van de aanpak van discriminatie en racisme. Daarbij baseren wij ons op door NewBizz in opdracht van Sportinnovator uitgevoerde marktverkenning,[10] en de door hen daarop gegeven toelichting tijdens interview 2. Dit betreffen de slimme technologieën die tot dusver in het kader van het project OVIVI aan bod zijn gekomen.[11]

Wij lichten deze technologieën per fase toe (paragraaf 3.1). Daarbij maken wij onderscheid tussen 1) het signaleren van discriminatie en racisme, 2) het identificeren van de betrokkenen en 3) het gebruik van de in fase 1 en 2 verzamelde gegevens ten behoeve van het opleggen van een sanctie aan de betrokkenen.

Vervolgens lichten wij toe welke partijen (in ieder geval) betrokken zijn bij de inzet van de technologieën (paragraaf 3.2).

Wij sluiten dit hoofdstuk af met een samenvattend overzicht van de verschillende type camera's die in dit rapport aan bod komen (paragraaf 3.3).

3.1 Mogelijke technologieën per fase

3.1.1 Fase 1 – Signaleren van discriminatie en racisme

Voor het signaleren van discriminatie en racisme kunnen slimme camera's en slimme microfoons worden ingezet, al dan niet gecombineerd met emotieherkenningstechnologie. Wij lichten hierna toe hoe deze slimme camera's en microfoons (kunnen) werken, evenals hoe emotieherkenningstechnologie kan werken.

Slimme camera's en microfoons

Op dit moment zijn BVO's op grond van de licentie-eisen van de KNVB verplicht het stadion te voorzien van een video-installatie. Deze video-installatie moet zo zijn opgesteld dat in ieder geval de toeschouwersvakken, de plaatsen waar fouilleringswerkzaamheden worden verricht, toegangspunten tot het stadion(terrein) en toegangswegen en het stadionplein in beeld kunnen worden gebracht. Ten minste één videocamera moet permanent op het bezoekersvak zijn gericht. Voorts stelt de KNVB kwaliteitseisen aan de beelden, onder andere de eis dat het mogelijk moet zijn op basis van de beelden personen te herkennen en dat datum en tijd permanent op de

[10] NewBizz B.V., 'Marktonderzoek ter bestrijding van racisme en discriminatie in voetbalstadions', 23 oktober 2020. Sportinnovator heeft ervoor gekozen dit onderzoek niet openbaar te maken en te verspreiden, omdat de uiteindelijke vorm niet overeenkomt met haar standaard.

[11] Volledigheidshalve merken wij daarbij op dat mogelijk ook andere (combinaties van) slimme technologieën kunnen worden ingezet ten behoeve van de aanpak van discriminatie en racisme in voetbalstadions. Wij beogen met deze toelichting dan ook geen uitputtend overzicht te geven van slimme technologieën die kunnen worden ingezet.

beelden moet zijn geregistreerd. Ook moet de bediening van de video-installatie vanuit de zogenoemde commandoruimte geschieden.[12]

Wij begrijpen dat de video-installaties die op dit moment worden ingezet door de BVO's veelal beveiligingscamera's betreffen en dat deze van wisselende kwaliteit zijn. Doorgaans ontbreekt daarbij de mogelijkheid om *live* discriminatie of racisme te signaleren, waardoor beelden achteraf moeten worden teruggekeken, al dan niet naar aanleiding van meldingen van mogelijke discriminatie of racisme die/dat zou hebben plaatsgevonden rondom een wedstrijd.

De inzet van slimme camera's of andere beeldopnameapparatuur (zoals scanners)[13] maakt het mogelijk om *live* discriminatie of racisme te signaleren. Voor de goede werking hiervan moet, zo begrijpen wij, het maken van beeldopnames worden gecombineerd met het maken van geluidsopnames.

Dat zou als volgt kunnen werken:

- Bij een wedstrijd in het stadion worden beeld- en geluidsopnames gemaakt.
- Het beeld en het geluid loopt synchroon.
- De camera's en microfoons[14] staan zo ingesteld dat deze bij indicaties van discriminatie of racisme kunnen inzoomen op de bron van die mogelijke discriminatie of dat mogelijke racisme.
    - Voor wat betreft de beeldopnames gaat het dan om opvallende bewegingen, houdingen, objecten (zoals spandoeken) en patronen.
    - Voor wat betreft geluid gaat het om opvallend(e) volume (bijvoorbeeld kreten of vuurwerk), frequentie en inhoud (zoals bepaalde woorden of zinnen die kunnen worden herkend met behulp van spraakherkenning[15]);
- Dergelijke opvallende beelden of geluiden kunnen vooraf worden ingesteld. In aanvulling daarop kan het systeem zichzelf leren dat bepaalde indicaties worden toegevoegd en/of verhoogde prioriteit krijgen. Het algoritme dat ten grondslag ligt aan de (software van de) camera's en microfoons kan dus (deels) zelflerend zijn.
- Concreet zullen een slimme camera en een slimme microfoon, die bijvoorbeeld een bereik hebben van een vak met 500 toeschouwers, op basis van de ingestelde (en eventueel ook aangeleerde) indicaties inzoomen op een kleinere groep toeschouwers die de bron zijn van de mogelijke discriminatie/het mogelijke racisme (het zgn. 'clusterniveau'). Van dat

[12] KNVB, 'Richtlijn licentie-eisen', seizoen 2020/'21 (laatst gewijzigd 24 september 2020), raadpleegbaar via: https://www.knvb.nl/downloads/bestand/2990/richtlijn-licentie-eisen-v27. Het gaat concreet om nummer I.13 op p. 32-33.

[13] Ten behoeve van de leesbaarheid spreken wij hierna van camera's, maar dit kan ook andere beeldopnameapparatuur zijn.

[14] Ten behoeve van de leesbaarheid spreken wij hierna van microfoons, maar dit kan ook andere geluidopnameapparatuur zijn.

[15] Spraakherkenning (herkenning van de inhoud) moet worden onderscheiden van stemherkenning (herkenning van de stem van een individualiseerbaar persoon; zie daarover paragraaf 3.1.2 hierna).

cluster zullen de beelden en geluiden dan ingezoomd worden opgenomen (een zgn. 'positie-recording' van de situatie).

- Dat gaat als volgt: er wordt een zgn. *grid* toegevoegd aan de microfoons. Op basis daarvan kan de audio worden opgenomen van het cluster waar de overtreding plaatsvindt. Ook de camera kan als het mogelijke discriminatie of racisme constateert inzoomen op een cluster. De camera en de microfoon hebben een sturende werking naar elkaar en een afhankelijkheid van elkaar.
- De slimme camera's zijn vervolgens (ook) in staat verder in te zoomen op een of enkele personen (zgn. 'pin pointing'). Dat gaat op basis van dezelfde principes als hiervoor beschreven.
- Voor slimme microfoons is het lastiger in te zoomen op een of enkele personen, omdat het geluid van personen die dicht op elkaar staan vermengd raakt, zeker bij de echo in een stadion (vgl. het geluid van een koor in een kerk, waarbij de individuele stemmen ook lastig zijn te onderscheiden).

Een oplossing waarbij handmatig wordt ingezoomd kan ook tot de mogelijkheden behoren. Dit betreft echter geen slimme technologie.

Emotieherkenningstechnologie

In aanvulling op de slimme camera's en microfoons kan emotieherkenningstechnologie worden ingezet. Wij begrijpen dat dergelijke technologie de sfeer kan herkennen op een bepaald moment. Het herkennen van emotie (sfeer), naast het herkennen van indicaties van discriminatie of racisme door slimme camera's en microfoons, kan bijdragen aan de signalering van discriminatie en racisme.

Dat zou als volgt kunnen werken:

- Naast de opname van beeld en geluid vindt er parallel een meting van emoties (sfeer) plaats.
- Het aanwezige geluid wordt continu voorzien van metadata over emotie. Dat kan zowel de emotie van een groep zijn of van een persoon.
- De huidige stand van de technologie kan vijf emoties herkennen: gelukkig, positief, neutraal, verdrietig en boos.
    - Daarmee zou bijvoorbeeld onderscheid kunnen worden gemaakt tussen, vrij vertaald, onschuldig bedoeld gedrag (Ajax-supporters die de term 'joden' als geuzennaam hanteren) en discriminerend of racistisch gedrag (het gebruik van diezelfde term op discriminerende of racistische wijze door de supporters van de tegenstander van Ajax).
- Deze emoties kunnen worden gemeten op basis van een neuraal netwerk. Het gaat daarbij om bijvoorbeeld vibraties van geluid en stemspanning.
- De gemeten emotie is daarbij een extra waarde die bijdraagt aan het al dan niet inzoomen van de beeldopname- en geluidopnameapparatuur op een bepaald cluster en vervolgens op een of enkele personen.

3.1.2 Fase 2 – Identificeren van de betrokkene

Nadat discriminatie of racisme is gesignaleerd zullen de daders ('betrokkene(n)') moeten worden geïdentificeerd, opdat er aan hen een sanctie kan worden opgelegd. Op dit moment gebeurt dat veelal handmatig.[16] Een slimme technologie die kan worden ingezet voor het (al dan niet deels) geautomatiseerd identificeren van betrokkenen betreft de inzet van gezichtsherkenningstechnologie. Hieronder lichten wij toe hoe die technologie kan worden ingezet.

Voorts bespreken wij andere slimme technologieën die kunnen worden ingezet ten behoeve van de identificatie van betrokkenen, te weten stemherkenning en stoelnummerregistratie.

Gezichtsherkenningstechnologie

Bij de inzet van gezichtsherkenningstechnologie zullen op basis van de beelden van de gesignaleerde discriminatie of het gesignaleerde racisme de betrokken personen worden geïdentificeerd. Daarvoor is vereist dat de (personen op de) betreffende beelden kunnen worden vergeleken met zogenoemd referentiemateriaal. Er moet, met andere woorden, reeds beeldmateriaal beschikbaar zijn van de aanwezigen in het stadion (de 'registratiestap'). De technologie is vervolgens in staat te identificeren wie de betrokkene is op basis van de biometrische kenmerken van deze persoon (de 'vergelijkingsstap').

Er zijn verschillende opties om de vergelijking op basis van biometrische gegevens te maken:

- Registratie bij de aanschaf van toegangskaarten en foto bij binnenkomst: voor het kopen van een toegangskaart moet de toeschouwer zich registreren. Hierdoor zijn de persoonsgegevens van degene die naar het stadion komt bekend. Bij binnenkomst in het stadion wordt de toegangskaart gescand (bijvoorbeeld door middel van een QR-code) en een foto gemaakt van de houder van de toegangskaart. Die foto wordt opgeslagen in combinatie met de aan de toegangskaart verbonden, geregistreerde persoonsgegevens. Deze persoonsgegevens zouden versleuteld kunnen worden opgeslagen. Op het moment dat er beelden van discriminerend of racistisch gedrag zijn, worden die beelden vergeleken (eventueel na versleuteling) met de bij de toegangspoorten gemaakte foto's. In het geval van een match worden de opgeslagen persoonsgegevens vrijgegeven.

- QR-code scannen en foto bij binnenkomst: bij de toegangspoorten scannen toeschouwers een QR-code. Op dat moment worden persoonsgegevens van de betreffende toeschouwer van zijn of haar telefoon

[16] In het verleden is, zo begrijpen wij, door sommige BVO's wel gebruik gemaakt van biometrie ten behoeve van de identificatie van betrokkenen.

gehaald, dan wel moet de toeschouwer zijn persoonsgegevens invullen. Tegelijkertijd wordt, net als bij de optie hierboven, op het moment dat de QR-code wordt gescand ook een foto gemaakt. Anders dan de optie hierboven hoeft bij deze optie geen registratie plaats te vinden van de persoonsgegevens van de toeschouwer voor de aanschaf van toegangskaarten, omdat persoonsgegevens rechtstreeks uit de telefoon van de toeschouwer worden afgeleid of ter plaatse worden ingevuld. Ook deze persoonsgegevens zouden versleuteld kunnen worden opgeslagen en vervolgens alleen kunnen worden vrijgegeven als sprake is van een match op basis van de beelden en de opgeslagen foto.

- De clubkaart en seizoenkaart: zowel bij de aanschaf van een clubkaart als bij de aanschaf van een seizoenkaart moet men zich registreren met naam en (pas)foto. De beelden van discriminatoir of racistisch gedrag kunnen worden vergeleken met de foto's die behoren bij de aangeschafte club- en seizoenkaarten. Deze mogelijkheid vergt dat − naast seizoenkaarthouders, die toegang hebben tot iedere thuiswedstrijd − alleen losse toegangskaarten kunnen worden gekocht door met naam geregistreerde clubkaarthouders. Een clubkaarthouder kan dan slechts een toegangskaart per wedstrijd kopen voor zichzelf.

Bij het voorgaande zijn wij ervan uitgegaan dat gezichtsherkenningstechnologie alleen wordt ingezet om bij discriminatie of racisme betrokken personen te identificeren. Van *real time* identificatie door middel van gezichtsherkenningstechnologie is dus geen sprake.

Stemherkenning?

Naast gezichtsherkenningstechnologie kan ook stemherkenningstechnologie worden ingezet ten behoeve van de identificatie van betrokken. Die technologie zou in combinatie met gezichtsherkenningstechnologie of andere identificatiemiddelen kunnen worden ingezet. De precieze werking van stemherkenningstechnologie en de wijze waarop die technologie zou kunnen worden ingezet voor de identificatie van betrokkenen is niet nader toegelicht in de marktverkenning.

Stoelnummerregistratie?

Een andere identificatiemogelijkheid kan worden bewerkstelligd door iedere toeschouwer zich te laten registeren, en vervolgens een stoelnummer toe te wijzen aan iedere toeschouwer ('preregistratie'). De bij de registratie verstrekte persoonsgegevens kunnen versleuteld worden opgeslagen.

De opnames van discriminatoir en racistisch gedrag kunnen vervolgens worden gekoppeld aan de locatie, en meer specifiek aan het stoelnummer/de stoelnummers, waar dit gedrag plaatsvindt. Daarna kunnen de persoonsgegevens van degene die op

de betreffende locatie moet hebben gezeten worden vrijgegeven, opdat (handmatig) kan worden nagegaan wie de betrokkenen zijn.

Onderdeel van stoelnummerregistratie door middel van preregistratie kan ook zijn dat een foto wordt gemaakt van de toeschouwer bij de toegang tot het stadion met het verkregen toegangsbewijs. Die foto kan mede worden gebruikt voor de identificatie van betrokkenen.

3.1.3 Fase 3 – Gebruik van de gegevens ten behoeve van sanctieoplegging

Het opleggen van een sanctie kan zowel een civielrechtelijk stadionverbod betreffen als bestraffing op grond van het strafrecht. Wij lichten hieronder toe hoe op dit moment gegevens betreffende een incident worden verwerkt ten behoeve van het opleggen van een sanctie en in hoeverre deze verdere verwerkingen veranderen als in fase 1 en/of 2 (een combinatie van) slimme technologie wordt ingezet.

Na een wedstrijd rapporteert een BVO in de Keten Voorziening Voetbal ('KVV') over het verloop van een wedstrijd. Eventuele ongeregeldheden, waaronder discriminatoir of racistisch gedrag dat zich heeft voorgedaan tijdens de wedstrijd, worden via dit systeem gemeld bij de KNVB. Daarbij worden de incidenten omschreven en de relevante gegevens, waaronder de verkregen beeld- en geluidopnames, ingeladen. Naar wij begrijpen, wordt ook de (vermoedelijke) identiteit van de betrokkene verwerkt. Voorts vermeldt de BVO in dit systeem wat de procedure is die zal (moeten) volgen. Dat kan het opleggen van een landelijk stadionverbod (door de KNVB) zijn. Of, als de KNVB daartoe niet overgaat of kan overgaan, het opleggen van een lokaal stadionverbod (door de BVO).

De politie treedt op tegen incidenten indien er aangifte wordt gedaan. Dat kan bijvoorbeeld een persoonlijke aangifte zijn, maar in de praktijk gaat het bij discriminatie of racisme gerelateerde aangiftes veelal om aangiftes van een stichting die opkomt voor de belangen van een bepaalde groep. Vervolgens kan de politie, en later het OM, de beeld- en geluidsopnames van de wedstrijd opvragen bij de BVO ten behoeve van de opsporing en vervolging.

Bij de inzet van slimme technologie op de hierboven beschreven wijze zal de werkwijze in fase 3 voor wat betreft de gesignaleerde incidenten (in fase 1) naar onze inschatting niet wijzigen. Verkregen opnames zullen, net als op dit moment het geval is, kunnen worden ingeladen in de KVV.

Dat is anders voor wat betreft de inzet van gezichtsherkenningstechnologie en/of andere slimme identificatietechnologie ten behoeve van het identificeren van de betrokkene(n) (in fase 2). In dat geval kan de BVO in de KVV aangeven wie de betrokkene is naar aanleiding van de technologie die wordt ingezet voor de identificatie. Dat roept de vraag op welke gegevens de BVO in dat geval opneemt in de KVV. Dat zou alleen de uitkomst kunnen zijn ("de betrokkene is persoon A") of ook de

gegevens die zijn gebruikt om tot die uitkomst te komen (de gebruikte beelden in combinatie met het gebruikte referentiemateriaal waaruit blijkt dat de betrokkene persoon A is). Daarbij kan een rol spelen welke partij uiteindelijk over zal gaan tot het opleggen van een sanctie.

Denkbaar is ook dat de aanklagende instantie in fase 3 gezichtsherkenningstechnologie en/of andere slimme identificatietechnologie inzet op basis van eigen databases met referentiemateriaal.

3.2 Betrokken partijen

Hieronder beschrijven wij de partijen die betrokken zijn bij het signaleren van discriminatie en racisme, het identificeren van de betrokkenen en de sanctieoplegging.

KNVB

De KNVB is verantwoordelijk voor een goed en ordentelijk verloop van de competitie. In dat kader stelt de KNVB onder meer kwaliteitseisen aan BVO's – zgn. licentie-eisen – om deel te kunnen nemen aan de door de KNVB georganiseerde competities betaald voetbal.[17] Deze eisen hebben onder meer betrekking op veiligheid, beveiliging en klantvriendelijkheid.[18]

De KNVB is in bepaalde gevallen bevoegd om een landelijk stadionverbod op te leggen. Zowel een BVO als het OM kunnen bij de KNVB melding doen van een toeschouwer die zich vermoedelijk schuldig heeft gemaakt aan het overtreden van de standaardvoorwaarden van de KNVB of die anderszins voetbalgerelateerd wangedrag heeft vertoond, zoals discriminatoir of racistisch gedrag. Indien de melding voldoende aanknopingspunten bevat, gaat de KNVB in beginsel over tot oplegging van een landelijk stadionverbod.[19]

BVO's

BVO's zijn verantwoordelijk voor de organisatie van de afzonderlijke wedstrijden en, in het verlengde daarvan, primair verantwoordelijk voor het ordentelijke verloop van die wedstrijden.[20] BVO's moeten zorgen voor de veiligheidsorganisatie in het stadion, waaronder voor een adequate stewardorganisatie conform de licentie-eisen van de KNVB. Onderdeel van de veiligheidsorganisatie is ook, zoals reeds toegelicht in paragraaf 3.1.1 hierboven, de inzet van videocamera's.

---

17 KNVB, 'Richtlijn licentie-eisen', seizoen 2020/'21 (laatst gewijzigd 24 september 2020), raadpleegbaar via: https://www.knvb.nl/downloads/bestand/2990/richtlijn-licentie-eisen-v27.

18 Ministerie van Veiligheid en Justitie (thans Ministerie van Justitie en Veiligheid), 'Kader voor beleid, voetbal en veiligheid', p. 49. Dit kader voor beleid is een bijlage bij Kamerstukken II 2010/11, 25 232, nr. 57.

19 Ministerie van Veiligheid en Justitie (thans Ministerie van Justitie en Veiligheid), 'Kader voor beleid, voetbal en veiligheid', p. 51.

20 Zie daarover uitgebreider: Ministerie van Veiligheid en Justitie (thans Ministerie van Justitie en Veiligheid), 'Kader voor beleid, voetbal en veiligheid', p. 53-54.

Indien personen zich schuldig hebben gemaakt aan voetbalgerelateerd wangedrag, waaronder discriminatie of racisme, dan gaat de BVO over tot rapportering daarvan aan de KNVB in de KVV. De KNVB kan op basis van die informatie overgaan tot oplegging van een landelijk stadionverbod. De BVO zelf kan ook overgaan tot oplegging van een lokaal stadionverbod, bijvoorbeeld als de KNVB geen aanleiding ziet voor een landelijk stadionverbod.

De veiligheid rondom (betaald)voetbalwedstrijden wordt voorafgaand aan een wedstrijd besproken in de zogenoemde "voetbalvierhoek", bestaande uit (afgevaardigden van) de betrokken BVO's, de gemeente, de politie en het OM. Tijdens de wedstrijd zitten afgevaardigden van (een deel van) deze partijen in de commandoruimte in het stadion (zie daarover ook licentie-eis I.02). Vaak betreffen dit in ieder geval de veiligheidscoördinatoren van de twee betrokken BVO's en veelal ook afgevaardigden van de gemeente en politie.

(Burgemeesters van) gemeenten

De burgemeester van de gemeente waarin het voetbalstadion is gelegen, is degene die een BVO toestemming verleent voor het spelen van voetbalwedstrijden door het afgeven van een veiligheidsverklaring (zie daarover ook licentie-eis I.01 van de KNVB).

De burgemeester draagt er zorg voor dat alle bestuursrechtelijke maatregelen die genomen kunnen worden om voetbalvandalisme te bestrijden in de APV zijn opgenomen, met uitzondering van de maatregelen die al in de Gemeentewet vastgelegd zijn.

Tevens is de burgemeester (eind)verantwoordelijk voor de handhaving van de openbare orde. In dat kader is de burgemeester ook degene met de hoogste beslissingsmacht en kan hij besluiten om wedstrijden te verbieden, van categorie te laten veranderen en om wedstrijden te laten stilleggen. Met betrekking tot die verantwoordelijkheid is de burgemeester, naast gemeentelijk bestuursorgaan, ook gezagsdrager over de politie. Hoewel wij de rol van de (burgemeesters van) gemeenten hier volledigheidshalve benoemen, heeft de burgemeester bij de signalering, identificatie of sanctieoplegging op de wijzen zoals die tot dusver is onderzocht geen wezenlijke rol. De gemeentelijke bevoegdheden blijven daarom in het vervolg van dit rapport onbesproken.

Politie

De taak van de politie is tweeledig: de openbare ordetaak en de taak inzake de strafrechtelijke handhaving van de rechtsorde. Eerstgenoemde taak heeft betrekking op de handhaving van de openbare orde rondom voetbalwedstrijden. Laatstgenoemde taak betreft de opsporing van strafbare feiten die zich tijdens een wedstrijd hebben voorgedaan. Voor dit rapport is met name de laatstgenoemde taak relevant, namelijk

de opsporing van daders wanneer aangifte wordt gedaan van discriminatie of racisme rondom een wedstrijd.

Openbaar Ministerie

Indien wordt overgegaan tot strafrechtelijke handhaving van discriminatoir of racistisch gedrag, dan komt ook het OM in beeld. Het OM kan overgaan tot vervolging van de verdachte van die strafrechtelijke gedraging.

Ook kan het OM bij de KNVB melding doen van een supporter die zich vermoedelijk schuldig heeft gemaakt aan het overtreden van de standaardvoorwaarden van de KNVB of aan ander voetbalgerelateerd wangedrag, wat kan leiden tot een landelijk stadionverbod.

3.3 Onderscheid verschillende camera's

Uit het voorgaande volgt dat in stadions verschillende slimme technologieën kunnen worden ingezet ten behoeve van het signaleren van discriminatie en racisme en het identificeren van de betrokkenen. In dat kader zijn verschillende type camera's genoemd. In het vervolg van dit rapport maken wij onderscheid tussen de volgende camera's:

- **(Gewone) camera's**: dit zijn de videocamera's die gewoonweg beeldopnames maken, zoals beveiligingscamera's. Dergelijke camera's zijn ook nu al op grond van de licentie-eisen van de KNVB verplicht in stadions van BVO's;
- **Slimme camera's**: dit zijn camera's die in staat zijn om op basis van beeld- en geluidopnames discriminatoir of racistisch gedrag te herkennen, daarop in te zoomen en vervolgens dat gedrag zowel in beeld als geluid kunnen vastleggen (zie paragraaf 3.1.1 hierboven);
- **Camera's m**et gezichtsherkenningstechnologie: dit betreffen camera's die in staat zijn om op basis van een beeldopname van een persoon de betreffende persoon te kunnen identificeren. De camera maakt daarbij een vergelijking tussen de persoon die wordt gefilmd en eerder verkregen referentiemateriaal (zie paragraaf 3.1.2 hierboven).

Denkbaar is dat slimme camera's (zie bullet 2) worden uitgerust met gezichtsherkenningstechnologie (zie bullet 3).

4 TOEPASSELIJKHEID VAN DE AVG: WORDEN ER PERSOONSGEGEVENS VERWERKT?

Voordat wordt toegekomen aan een inhoudelijke beoordeling van de toelaatbaarheid van de inzet van slimme technologieën in voetbalstadions, is allereerst van belang om vast te stellen of en zo ja, in hoeverre de AVG en/of eventuele aanvullende sectorale gegevensbeschermingswetgeving van toepassing is.

4.1 Juridisch kader

4.1.1 Materieel toepassingsgebied: het verwerken van persoonsgegevens

De AVG is van toepassing op de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.[21]

Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbaar natuurlijk persoon. Als een identificeerbaar persoon wordt beschouwd iedere informatie die direct (bijvoorbeeld een naam, adres of telefoonnummer), dan wel indirect (bijvoorbeeld een Burgerservicenummer (‘BSN’)) herleidbaar is tot een natuurlijke persoon.[22] Van een persoonsgegeven is aldus snel sprake.

Voor de vraag of sprake is van identificeerbaarheid moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is, dan wel door derden in te zetten zijn, om de persoon te identificeren. Daarbij moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen (denk aan de toenemende rekenkracht van computers en het groeiende aantal beschikbare hulpmiddelen).[23]

4.1.2 Anonieme gegevens en gepseudonimiseerde persoonsgegevens

De AVG is niet van toepassing op gegevens die zodanig anoniem zijn (gemaakt) dat de persoon waarop ze betrekking hebben niet (meer) identificeerbaar is. In dat geval is er, met andere woorden, geen sprake meer van persoonsgegevens. Er bestaat veel discussie over de vraag wanneer sprake is van anonieme gegevens.

---

21 Zie artikel 2, lid 1, AVG.

22 In definitie van het begrip persoonsgegeven in de AVG wordt gesproken over identificatie “met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon”.

23 Overweging 26 van de AVG.

De discussie of sprake is van anonieme gegevens richt zich veelal op de vraag of versleutelde[24] en gehashte[25] gegevens anonieme gegevens betreffen. De gezaghebbende Artikel 29-Werkgroep (inmiddels: de European Data Protection Board ('EDPB')) – waarin de Europese privacytoezichthouders zijn verenigd – hanteert als uitgangspunt dat pas gesproken kan worden van 'anonieme gegevens' indien iedere mogelijkheid tot identificatie van de betrokkene onherroepelijk is uitgesloten.[26] Daarbij neemt de Artikel 29-Werkgroep tot uitgangspunt dat herleidbaarheid, koppelbaarheid en deduceerbaarheid (redelijkerwijs) onmogelijk moet zijn.[27] De Europese privacytoezichthouders zijn van oordeel dat de versleuteling en/of hashing van persoonsgegevens (veelal) moet worden gezien als een manier om persoonsgegevens te pseudonimiseren, en dus als een beveiligingsmaatregel.[28] Gepseudonimiseerde persoonsgegevens vallen daarmee onverkort onder de reikwijdte van de AVG.[29]

Reden daarvoor is volgens de Artikel 29-Werkgroep dat – anders dan bij anonimisering, waarbij *elke* mogelijkheid tot identificatie onomkeerbaar wordt uitgesloten – bij pseudonimisering de kans op identificatie blijft bestaan. De inzet van pseudonimisering heeft enkel tot gevolg dat de koppelbaarheid van een dataset aan de oorspronkelijke dataset wordt *beperkt*. Degene die versleuteling en/of hashing heeft toegepast, houdt echter de beschikking over de encryptiesleutel en/of de oorspronkelijke gegevens. In de optiek van de Europese privacytoezichthouders blijft het daardoor voor de sleutelhouder mogelijk om de versleuteling/hashing van de persoonsgegevens terug te draaien. Zolang de oorspronkelijke gegevens en de encryptiesleutel worden bewaard, blijft bovendien het risico bestaan dat (onbevoegde) derden de gegevens kunnen de-pseudonimiseren, bijvoorbeeld doordat zij de encryptiesleutel in handen krijgen (al dan niet door hacks, brutekrachtaanvallen of datalekken). Ook dit vormt een zelfstandig risico op herleidbaarheid tot de betrokkenen.

Het maakt volgens de Artikel 29-Werkgroep overigens geen verschil of de encryptiesleutel en/of de oorspronkelijke gegevens worden bewaard door een vertrouwde derde partij (een zogenoemde Trusted Third Party ('TTP')). In die situatie wordt de herleidbaarheid tot het identificeren van de betrokkenen volgens de Artikel 29-Werkgroep eveneens onvoldoende uitgesloten.

---

24 Versleuteling houdt in dat de persoonsgegevens door middel van encryptie met een geheime sleutel worden beveiligd.

25 Hashing houdt in dat persoonsgegevens van een willekeurige omvang door middel van een hashfunctie worden omgevormd naar reeks van een vaste grootte. De persoonsgegevens zijn dus niet meer zichtbaar, tenzij de gehashte gegevens bijv. door middel van brutekrachtaanvallen zouden worden herberekend.

26 In deze groep waren (tot en met 25 mei 2018) de Europese privacytoezichthouders verenigd. De groep bracht onder meer adviezen uit over de interpretatie van begrippen in de privacyrichtlijn en de Wbp. De opinies van deze groep waren en zijn nog steeds zeer gezaghebbend. Sinds 25 mei 2018 heeft de EDPB de taken van de Artikel 29-Werkgroep overgenomen. De eerdere adviezen van de Artikel 29-Werkgroep zijn door de EDPB bekrachtigd.

27 Zie Artikel 29-Werkgroep, Advies 5/2014 over anonimiseringstechnieken, WP 216, p. 24; zie ook: EDPB, Richtsnoeren 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19, vastgesteld op 21 april 2020, nr. 15.

28 Zie Artikel 29-Werkgroep, Advies 5/2014 over anonimiseringstechnieken, WP 216, p. 1. Zie ook artikel 32, eerste lid, aanhef en onder a AVG.

29 Zie daarover ook recent: EDPB, '10 misunderstandings related to anonymisation', 27 april 2021. Raadpleegbaar via: https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf.

Het standpunt van de (Europese) privacytoezichthouders lijkt zich uit te strekken tot in ieder geval een groot aantal, maar mogelijk ook wel alle hashing- en versleutelingstechnieken. Tegelijkertijd sluiten zij anonimisering door hashing- of versleutelingstechnieken niet geheel uit.[30] Een dataset kan mogelijk als anoniem worden beschouwd wanneer extra stappen worden ondernomen in aanvulling op de pseudonimisering, bijvoorbeeld door het wegnemen van gegevens (attributen) en generaliseren, de oorspronkelijke gegevens te verwijderen of op zijn minst samen te voegen tot een hoog aggregatieniveau.[31] Duidelijkheid over wanneer aan deze (aanvullende) voorwaarden is voldaan, is door de Europese privacytoezichthouders vooralsnog niet gegeven.

Zolang deze onduidelijkheid blijft bestaan, verdient het aanbeveling om er − en dat wordt in dit rapport ook gedaan − van uit te gaan dat het hashen of versleutelen van persoonsgegevens slechts leidt tot pseudonimisering, ook al is daar in bepaalde gevallen discussie over mogelijk.[32] Dat betekent ook dat in dit rapport zekerheidshalve wordt aangenomen dat voor zover er persoonsgegevens worden verwerkt, de AVG op die persoonsgegevens van toepassing is, óók na de inzet van hashing- of versleutelingstechnieken. Evenwel kan pseudonimisering door middel van hashing- of versleutelingstechnieken in sommige gevallen een belangrijke te nemen beveiligingsmaatregel zijn.

4.1.3 Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn persoonsgegevens die naar hun aard gevoelig zijn. Het gaat bijvoorbeeld om gegevens over iemands gezondheid, ras, etniciteit, politieke opvatting of seksuele gerichtheid. Ook biometrische gegevens die worden verwerkt met het oog op de unieke identificatie van een persoon betreffen bijzondere persoonsgegevens.[33]

Op de verwerking van bijzondere persoonsgegevens is een strikt regime van toepassing. In artikel 9 AVG is bepaald dat het verboden is om bijzondere persoonsgegevens te verwerken, tenzij de verwerking kan worden gebaseerd op een doorbrekingsgrond (ook wel: uitzonderingsgrond; zie daarover paragraaf 6.1.4 hierna).

---

30 Zie bijvoorbeeld https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens ten aanzien van hashing: "Gehashte persoonsgegevens zijn meestal niet anoniem." (onderstreping toegevoegd).

31 Zie Artikel 29-Werkgroep, Advies 5/2014 over anonimiseringstechnieken, WP 216, p. 24-25 en p. 34.

32 Er is discussie mogelijk, aangezien (lagere) rechtspraak bestaat die enige steun biedt voor de opvatting dat het onomkeerbaar dubbel pseudonimiseren van persoonsgegevens ertoe kan leiden dat niet meer gesproken kan worden van persoonsgegevens (Rb. Midden Nederland 2 augustus 2017, ECLI:NL:RBMNE:2017:4011, rov. 4.10-4.11). Aan deze rechtspraak lijkt echter geen doorslaggevende betekenis te kunnen worden toegekend, aangezien in deze rechtspraak met enige nadruk wordt benadrukt dat voor de vaststelling of er inderdaad wél of géén sprake is van persoonsgegevens 'een gedetailleerde beoordeling' nodig is 'van de precieze inhoud van hetgeen door een instantie aan gegevens wordt geregistreerd en de wijze van registratie, alsmede een adequaat zicht op de zich steeds verder ontwikkelende (informatie-)technologische middelen die ter identificering van de betrokken persoon kunnen worden ingezet'.

33 Zie artikel 9, eerste lid, AVG voor een limitatieve opsomming van de persoonsgegevens die als bijzondere persoonsgegevens kwalificeren.

Ook de Wet politiegegevens (‘Wpg’) en de Wet justitiële en strafvorderlijke gegevens (‘Wjsg’) bevatten bepalingen over de toelaatbaarheid van de verwerking van bijzondere persoonsgegevens, waaronder biometrische gegevens. Dat kan relevant zijn voor het geval de politie respectievelijk het OM biometrische gegevens gaat verwerken.

4.1.4 Strafrechtelijke persoonsgegevens

In artikel 10 AVG zijn regels gesteld voor “persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen” (‘strafrechtelijke persoonsgegevens’). In artikel 1 UAVG is daaraan toegevoegd dat ook persoonsgegevens “betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag” gegevens van strafrechtelijke aard zijn. In dit rapport duiden we ook deze gegevens aan als strafrechtelijke gegevens.

Het is niet altijd duidelijk wat wel en niet als strafrechtelijke persoonsgegevens kwalificeren, bijvoorbeeld als het gaat om gegevens over een verdachte die (nog) niet is veroordeeld.

In de parlementaire geschiedenis bij artikel 16 Wet bescherming persoonsgegevens (‘Wbp’) dat was gebaseerd op artikel 8, vijfde lid, Privacyrichtlijn, de voorganger van het huidige artikel 10 AVG) is daarover opgemerkt dat het bij strafrechtelijke gegevens gaat om gegevens die “zowel op veroordelingen als op min of meer gegronde verdenkingen” betrekking hebben. Dit wordt op de volgende wijze toegelicht:

> “Veroordelingen betreffen gegevens waarbij de rechter, al dan niet onherroepelijk, strafrechtelijk gedrag heeft vastgesteld. Bij verdenkingen gaat het om concrete aanwijzingen jegens een bepaalde persoon. Het begrip strafrechtelijk gegevens omvat mede gegevens omtrent de toepassing van het formele strafrecht, bijvoorbeeld het gegeven dat iemand is gearresteerd of dat tegen hem proces-verbaal is opgemaakt wegens een bepaald vergrijp. De bepaling heeft geen betrekking op de verwerking van persoonsgegevens gericht op de vaststelling van mogelijk strafbaar gedrag, bij voorbeeld door het volgen van trends.”[34]

Uit de rechtspraak over het begrip kan worden opgemaakt dat het moet gaan om gegevens die een zwaardere verdenking opleveren dan een redelijk vermoeden van schuld.

Zie bijvoorbeeld:

- Gerechtshof 28 april 2020, ECLI:NL:GHARL:2020:3374, rov. 5.26 e.v.:

[34] Zie Kamerstukken II 1997/98, 25 892, nr. 3, p. 102 en 118.

> "(…) In dit geval gaat het om verwerking van een gegeven die bestaat uit een code. De Huismeesters geeft via de signaleringsmodule aan Woonurgentie Groningen een 'code 2' door. Die code is als zodanig geen strafrechtelijk gegeven. Deze code staat voor 'hennep' en is evenmin op zichzelf een strafrechtelijk gegeven. In de context van de signaleringsmodule en het bedoelde gebruik daarvan geeft De Huismeesters met 'code 2' door dat vanwege de aanwezigheid van hennepplanten in de van haar gehuurde woning de huurovereenkomst met [appellante] is beëindigd. Dat gegeven - de civielrechtelijke beëindiging van de huurovereenkomst vanwege hennepteelt in de woning - houdt op zichzelf evenmin in een gegeven van strafrechtelijke aard. Onder bijkomende feiten en/of omstandigheden kan uit de aanduiding 'hennep' - waarmee aldus civielrechtelijk bezien ongeoorloofde hennepteelt is bedoeld - volgen dat naast dat civielrechtelijk ongeoorloofd handelen (ook) sprake is van strafrechtelijk verwijtbaar handelen. Dat is echter naar het oordeel van het hof onvoldoende om in dit geval de verwerking van een code 2 aan te merken als een strafrechtelijke persoonsgegeven als hiervoor bedoeld. Of [appellante] strafrechtelijk is of wordt vervolgd en is of zal worden veroordeeld, volgt ook niet zonder meer uit de enkele (civielrechtelijk ongeoorloofde) aanwezigheid van een hennepplantage in de woning, laat staan uit de verwerking van 'code 2', en dit te minder gelet op de door [appellante] betwiste verantwoordelijkheid ter zake. Dat de code per saldo wel duidt op ongewenst huurdersgedrag maakt dit niet anders. De slotsom is dat het hof [appellante] niet volgt in haar betoog dat in haar geval voor verwerking van haar persoonsgegevens in de signaleringsmodule de strengere regels van artikel 10 AVG gelden. Het verwerken van de gegevens van [appellante] door De Huismeesters ten behoeve van derden dient dan ook getoetst te worden aan het bepaalde in artikel 6 AVG."
>
> Zie ook:
>
> - Rb. Rotterdam 6 januari 2020, ECLI:NL:RBROT:2020:211, rov. 4.6 en 4.8; en
> - HR 29 mei 2009, ECLI:NL:HR:2009:BH4720, r.o. 4.2 e.v.

In een uitspraak uit 2019 heeft het Hof Den Haag overwogen dat een civielrechtelijk contactverbod niet als strafrechtelijk persoonsgegeven als bedoeld in artikel 10 AVG kwalificeert. Daarvoor moet ten minste sprake zijn van maatregelen met een punitief karakter, wat bij een civielrechtelijk contactverbod niet het geval is.

> Zie Hof Den Haag 24 december 2019, ECLI:NL:GHDHA:2019:3539, rov. 4.23:
>
> "Een door de civiele rechter opgelegd contactverbod kan, anders dan Appellant betoogt, niet worden aangemerkt als een persoonsgegeven betreffende strafrechtelijke veroordelingen en strafbare feiten in de zin van artikel 10 AVG. De verwijzing naar het strafrecht impliceert dat het tenminste moet gaan om maatregelen met een punitief karakter. Een civielrechtelijk contactverbod heeft geen punitief karakter. Het feit dat de Nederlandse wetgever in artikel 1 van de UAVG heeft bepaald dat onder het begrip persoonsgegevens van strafrechtelijke aard mede vallen persoonsgegevens

betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag maakt dat niet anders. Het begrip persoonsgegeven betreffende strafrechtelijke veroordelingen en strafbare feiten in de zin van artikel 10 AVG is een Unierechtelijk begrip dat autonoom moet worden uitgelegd. De AVG geeft de lidstaten niet de mogelijkheid een eigen, ruimere invulling te geven aan dat begrip."

4.1.5 Wanneer is sprake van een verwerking (van persoonsgegevens)?

Bij de vraag naar de materiële toepasselijkheid van de AVG is ook van belang of persoonsgegevens worden *verwerkt*. Een verwerking is iedere bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens. Dit betreft een zeer ruim begrip. Als voorbeelden noemt artikel 4, tweede lid, AVG onder meer het verzamelen, opslaan, bijwerken en doorzenden van persoonsgegevens.[35] Ook het enkel bezoeken en/of analyseren van persoonsgegevens betreft een verwerking in de zin van de AVG.

4.1.6 Zijstap: sectorale gegevensbeschermingswetten

De AVG is niet van toepassing op de verwerking van persoonsgegevens "door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met in begrip van de bescherming tegen en voorkoming van gevaren voor de openbare veiligheid".[36] Deze verwerkingen worden gereguleerd door Richtlijn (EU) 2016/680,[37] die in de Wpg en de Wjsg zijn geïmplementeerd.

Dat betekent dat voor zover de persoonsgegevens die worden verwerkt met de slimme technologie in voetbalstadions kwalificeren als politiegegeven of als justitieel of strafvorderlijk gegeven, de Wpg respectievelijk de Wjsg van toepassing is in plaats van de AVG. Gelet daarop is voor een privacybeoordeling van in te zetten slimme technologie van belang onderscheid te maken tussen persoonsgegevens enerzijds en politiegegevens, justitiële gegevens en strafvorderlijke gegevens anderzijds. Wij lichten deze laatste drie begrippen daarom hieronder kort toe:

- Een politiegegeven is, kort gezegd, elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak.[38]

---

35 Zie voor de volledige opsomming artikel 4, tweede lid, AVG: "verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens."

36 Artikel 2, tweede lid, aanhef en onder d, AVG.

37 Richtlijn (EU) 2016/680 bescherming natuurlijke personen i.v.m. verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op voorkoming, onderzoek, opsporing en vervolging van strafbare feiten of tenuitvoerlegging van straffen, en vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ.

38 Zie artikel 1, aanhef en onder a, Wpg: "In deze wet en de daarop berustende bepalingen wordt verstaan onder: a. politiegegeven: elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4 van de Politiewet 2012, met uitzondering van: −de uitvoering van wettelijke voorschriften anders dan de Wet administratiefrechtelijke handhaving verkeersvoorschriften; −de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in artikel 1, eerste lid, onderdeel i, onder 1° en artikel 4, eerste lid, onderdeel f, van de Politiewet 2012;".

- Justitiële gegevens zijn "bij algemene maatregel van bestuur te omschrijven persoonsgegevens of gegevens over een rechtspersoon inzake de toepassing van het strafrecht of de strafvordering, die in een gegevensbestand zijn of worden verwerkt".[39] Het gaat hierbij om gegevens die worden geregistreerd ten aanzien van bepaalde strafbeschikkingen. In artikel 5 en 6 van het Besluit justitiële en strafvorderlijke gegevens ('Bjsg') is bepaald welke gegevens worden geregistreerd en in dat kader als justitieel gegeven worden aangemerkt.

- Strafvorderlijke gegevens zijn, kort gezegd, persoonsgegevens of gegevens over een rechtspersoon die het openbaar ministerie verwerkt in het kader van een strafvorderlijk onderzoek.[40]

4.2 De verwerking van persoonsgegevens met de slimme technologieën in voetbalstadions

Hieronder wordt per fase besproken of persoonsgegevens, bijzondere persoonsgegevens en/of strafrechtelijke persoonsgegevens worden verwerkt. Tot slot staan wij stil bij eventuele politiegegevens, justitiële of strafvorderlijke persoonsgegevens die worden verwerkt.

4.2.1 Fase 1 – Signaleren van discriminatie en racisme

Persoonsgegevens

Opnames van beelden, geluiden en/of emoties van toeschouwers in een voetbalstadion betreffen persoonsgegevens van de desbetreffende personen. (Onder andere) het opnemen, raadplegen en opslaan van deze opnames betreffen verwerkingen van persoonsgegevens. Deze verwerkingen zullen ook steeds geautomatiseerd zijn. De AVG is dan ook van toepassing op deze verwerkingen.[41]

Bijzondere persoonsgegevens

Beeldopnames kunnen voorts bijzondere persoonsgegevens bevatten, zoals gegevens waaruit ras of etnische afkomst of religieuze of levensbeschouwelijke overtuigingen blijken. Ook kunnen beeldopnames gezondheidsgegevens bevatten. Evenwel kwalificeert niet elke beeldopname waarop personen zichtbaar zijn zonder meer als gegevens betreffende ras, etniciteit, gezondheid of religie.

---

39 Artikel 1, aanhef en onder a, Wjsg.

40 Zie artikel 1, aanhef en onder b, Wjsg: "In deze wet en de daarop rustende bepalingen wordt verstaan onder: (…) b. strafvorderlijke persoonsgegevens: persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het openbaar ministerie in een strafdossier of langs geautomatiseerde weg in een gegevensbestand verwerkt"

41 Wij gaan ervan uit dat de verwerkingen ook steeds binnen het territoriale toepassingsgebied van de AVG vallen (artikel 3 AVG).

Zowel de AP als de EDPB[42] hebben in beleid[43] respectievelijk richtsnoeren[44] aangegeven dat het filmen van een persoon niet zonder meer leidt tot de verwerking van bijzondere persoonsgegevens. De AP legt op haar website uit dat beeldmateriaal niet kwalificeert als bijzondere persoonsgegevens indien:[45]

1. het verkrijgen van dat beeldmateriaal niet is gericht op ras, etniciteit, religie of gezondheid; en
2. het niet te voorzien is dat er op basis van het beeldmateriaal onderscheid gaat worden gemaakt naar ras, etniciteit, religie of gezondheid; en
3. onvermijdelijk is dat dergelijke gegevens worden verwerkt bij het maken van het beeldmateriaal.

Pas als het maken van beeldopnames is gericht op bijzondere persoonsgegevens en/of op basis van de opnames onderscheid zal worden gemaakt naar ras, etniciteit, religie of gezondheid, moet ervan uit worden gegaan dat de beelden kwalificeren als bijzondere persoonsgegevens. De AP noemt in dat kader in haar beleidsregels dat indien de verwerking van (bijzondere persoonsgegevens op) camerabeelden *identificatie* tot doel heeft, deze beelden als een rasgegeven worden aangemerkt.[46] Hoewel dat niet expliciet in de beleidsregels staat, lijkt zij daarmee te doelen op de situatie dat het primaire doel van beeldopnames is om op basis van de beelden personen te identificeren. Dat leiden wij af uit de omstandigheid dat de AP de inzet van beveiligingscamera's in winkels, met als doel de beveiliging van personen en goederen, niet als verwerking van bijzondere persoonsgegevens kwalificeert,[47] terwijl deze beelden vanzelfsprekend ook kunnen en zullen worden gebruikt om personen, die strafbare feiten plegen en waarvan beelden zijn gemaakt, achteraf te identificeren.

Relevant lijkt dus te zijn of het primaire doel van de inzet van camera's al dan niet is gelegen in identificatie van personen. Zodra dat wel het geval is, bijvoorbeeld bij camera's met gezichtsdetectie of gezichtsherkenningstechnologie, is sprake van de verwerking van bijzondere persoonsgegevens. Het kan dan gaan om rasgegevens,[48]

---

42 Dit betreft het overleg- en adviesorgaan waarin de privacytoezichthouders uit de verschillende lidstaten van de Europese Unie zijn verenigd (artikel 68 t/m 76 AVG).

43 AP, 'Cameratoezicht. Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens', 28 januari 2016 (raadpleegbaar via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf), p. 25-27.

44 EDPB, 'Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur', 29 januari 2020 (raadpleegbaar via: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf), p. 18 en in het bijzonder randnummers 62 respectievelijk 64.

45 Zie www.autoriteitpersoonsgegevens.nl > onderwerpen > foto en film > beeldmateriaal. Zie ook de hiervoor in paragraaf 4.2.1 (in de voetnoten) aangehaalde beleidstukken. Zie voorts conclusie A-G Machielse, 16 mei 2017, ECLI:NL:PHR:2017:547.

46 AP, 'Cameratoezicht. Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens', p. 26.

47 AP, 'Cameratoezicht. Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens', p. 26-27.

48 AP, 'Cameratoezicht. Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens', p. 51: "Ten aanzien van camera's met gezichtsdetectie wordt nog het volgende opgemerkt. Dergelijke camera's identificeren personen aan de hand van gegevensbestanden met unieke gezichtskenmerken. Aangezien het op deze wijze dus mogelijk is om een persoon te identificeren, zijn ook de gezichtskenmerken in de bestanden persoonsgegevens in de zin van de Wbp. Voorts geldt dat verwerkingen door middel van dit soort camera's veelal identificatie tot doel heeft. Dit betekent dat de AP de camerabeelden dan aanmerkt als rasgegevens in de zin van artikel 16 en

maar ook om biometrische gegevens als met behulp van een specifieke technische verwerking personen kunnen worden geïdentificeerd (zoals bij gezichtsherkenningstechnologie).[49]

Beeldopnames die bij een wedstrijd worden gemaakt in een stadion ten behoeve van het signaleren van discriminatoir of racistisch gedrag, hoeven onzes inziens niet te kwalificeren als bijzondere persoonsgegevens. De camera's worden ingezet met het primaire doel om ongewenst gedrag te signaleren. Dat het beeldmateriaal in een later stadium mogelijk ook zal worden gebruikt voor de identificatie van daders doet daar, naar analogie van de inzet van beveiligingscamera's in winkels, niet aan af.

Daarbij achten wij ook relevant dat het beeldmateriaal niet gericht is op het vastleggen van bijzondere kenmerken van de toeschouwers (het eerste vereiste), maar op het signaleren van mogelijk discriminatoir of racistisch handelen. Dat discriminatoire of racistische handelen kan vanzelfsprekend wél betrekking hebben op ras, etniciteit, religie of gezondheid. Maar: het gaat dan om ras, etniciteit, religie en/of gezondheid van een ander dan van degene die op de opnames zichtbaar is. De opnames zullen dan ook in de regel geen bijzondere persoonsgegevens bevatten van de betrokken toeschouwers (lees: degenen die zichtbaar zijn op het beeld).

Ook wordt op voorhand niet voorzien dat op basis van het beeldmateriaal onderscheid zal worden gemaakt naar ras, etniciteit, religie of gezondheid (het tweede vereiste). Voorts is het naar onze inschatting bij het maken van beeldopnames onvermijdelijk dat bepaalde kenmerken betreffende ras, etniciteit, religie en/of gezondheid van toeschouwers in beeld worden gebracht (het derde vereiste).

Wij vinden nog steun voor het uitgangspunt dat de verwerking van beeldmateriaal van de toeschouwers niet vanzelfsprekend moet worden beschouwd als de verwerking van bijzondere persoonsgegevens in overweging 51 van de AVG. Daaruit volgt dat de verwerking van foto's niet systematisch mag worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens, anders dan wanneer foto's worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken. In dat laatste geval is sprake van biometrische gegevens en daarmee in die zin sprake van bijzondere persoonsgegevens (zie daarover paragraaf 4.2.2 hierna), maar dus niet puur omdat (bijvoorbeeld) een kenmerk als ras op het beeld zichtbaar is.[50] Deze overweging uit de

18 Wbp. De verwerking van rasgegevens is verboden behoudens de uitzonderingen die de Wbp noemt in artikel 17 tot en met 23."

[49] Ten tijde van de beleidsregels van de AP inzake cameratoezicht was nog de (op de Europese privacyrichtlijn gebaseerde) Wbp in plaats van de AVG van toepassing. In de Wbp waren biometrische gegevens nog niet aangemerkt als bijzondere persoonsgegevens. Dat kan verklaren waarom de AP in het citaat in de voorgaande voetnoot verwijst naar rasgegevens voor de conclusie dat bij de inzet van camera's voor identificatiedoeleinden sprake is van bijzondere persoonsgegevens, en niet (ook) naar biometrische gegevens.

[50] Zie daarover ook H. de Vries, Tekst en commentaar Privacy- en gegevensbeschermingsrecht, art. 9, aant. 1: "Uit een foto zou het ras van een persoon kunnen worden afgeleid. Echter, foto's worden, anders dan onder de Wbp het geval was, niet begrepen onder het begrip ras. In de considerans is uiteengezet dat verwerking van foto's niet systematisch mag worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens, aangezien foto's alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of

AVG over foto's zou evengoed kunnen gelden voor ander beeldmateriaal, zoals camerabeelden, althans, wij zien niet in waarom deze overweging niet in gelijke zin geldt voor ander beeldmateriaal.

De verwerking van opnames van emotie kwalificeren naar ons oordeel niet als bijzondere persoonsgegevens.

> Ten overvloede: Een belangrijk aandachtspunt bij de inzet van slimme technologie is dat voor het ontwikkelen en trainen van slimme technologie uiteraard ook persoonsgegevens vereist zijn, met name beelden en geluiden van personen die discriminatoir of racistisch gedrag vertonen. Ook ten aanzien van dit trainingsproces menen wij dat geen sprake is van de verwerking van bijzondere persoonsgegevens, althans niet vanwege de enkele omstandigheid dat daarbij beelden worden gebruikt waaruit toevalligerwijs ook ras, etniciteit, religie of gezondheid kan worden afgeleid.

Strafrechtelijke persoonsgegevens

Vraag is of met de inzet van slimme opnametechnologie sprake is van de verwerking van strafrechtelijke persoonsgegevens. Daarbij is van belang dat de in te zetten slimme opnametechnologie in staat kan zijn om discriminatie of racisme te herkennen, en op basis daarvan zal inzoomen op de mogelijke daders.

Het valt niet uit te sluiten dat met de inzet van slimme technologie strafrechtelijke persoonsgegevens worden verwerkt. Persoonsgegevens van strafrechtelijke aard betreffen persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de AVG, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag. Daarvan is – kort gezegd - sprake als uit de beelden zodanige concrete feiten en omstandigheden blijken dat zij een bewezenverklaring van een strafbaar feit kunnen dragen, waarbij als maatstaf dient te worden genomen dat de vastgestelde gedragingen een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren.[51] Het strafbare discriminerend of racistisch gedrag dient in voldoende mate vast te staan.

Aangezien de inzet van slimme technologie specifiek tot doel heeft om dergelijk gedrag te signaleren en identificeren, zullen voetbalclubs niet kunnen uitsluiten dat bij de inzet van slimme technologie beelden worden vastgelegd die een dergelijke (strafrechtelijke) verdenking kunnen dragen.

---

authenticatie van een natuurlijke persoon mogelijk maken (overweging 51). Uit de gebruikte bewoordingen zou men kunnen opmaken dat foto's uitsluitend als biometrische gegevens kunnen worden aangemerkt en in geen geval als een ander bijzonder gegeven. Echter, de toelichting laat ruimte voor een ruimere uitleg: foto's mogen niet systematisch als bijzondere persoonsgegevens worden aangemerkt, maar onder omstandigheden wel, afhankelijk van het oogmerk van de gebruiker om onderscheid te maken, bijvoorbeeld naar ras (zie aant. 2 bij art. 25 UAVG)."

[51] Zie o.a. Rb. Den Haag 12 januari 2017, ECLI:NL:RBDHA:2017:264, rov. 4.12-14; Rb. Midden-Nederland 20 februari 2017, ECLI:NL:RBMNE:2017:805, rov. 4.8 en tot slot Rb. Amsterdam 22 maart 2018, ECLI:NL:RBAMS:2018:3354 en ECLI:NL:RBAMS:2018:3355, rov. 4.5.

4.2.2 Fase 2 − Identificeren van de betrokkene

Persoonsgegevens

Voor de identificatie van personen kan, zoals toegelicht in paragraaf 3.1.2, gebruik worden gemaakt van gezichtsherkenningstechnologie. In dat geval worden 1) vooraf de personen met beeldopname geregistreerd die als toeschouwer een wedstrijd gaan bijwonen, en 2) in het geval van een voorval de beelden van de betrokkenen vergeleken met de vooraf geregistreerde beeldopnames. Zowel bij de registratiestap als in de vergelijkingsstap is sprake van de geautomatiseerde verwerking van persoonsgegevens. De AVG is daarop van toepassing.

Wij wijzen erop dat ook bij het versleuteld opslaan van de persoonsgegevens die bij de registratiestap door de BVO worden verzameld, sprake is van de verwerking van persoonsgegevens. Dat geldt in ieder geval voor het moment waarop de persoonsgegevens worden verzameld en voor het moment waarop in verband met een match tussen de beelden van een incident en het referentiemateriaal (de voorafgaand aan een wedstrijd genomen of aangeleverde foto) de persoonsgegevens die horen bij de vooraf vastgelegde foto worden ontsleuteld. Er moet evenwel ook van uit worden gegaan dat het versleuteld opgeslagen houden van de geregistreerde persoonsgegevens, ondanks de toegepaste versleutelingsmethodiek, een verwerking van persoonsgegevens betreft (zie daarover paragraaf 4.1.2 en 4.1.5).

In paragraaf 3.1.2 is ook gewezen op de mogelijkheid om betrokkenen te identificeren op basis van een preregistratie gekoppeld aan stoelnummer. Identificatie vindt dan plaats door de locatie, en meer specifiek de stoelnummers, van het vastgelegde incident te koppelen aan de persoonsgegevens die vooraf zijn geregistreerd voor die stoelnummers. Dat betreft dan een automatische verwerking van persoonsgegevens waarop de AVG van toepassing is. Eventuele versleuteling van de geregistreerde persoonsgegevens tot het moment waarop er een incident plaatsvindt, maakt dat niet anders (vgl. hetgeen wij reeds hierboven opmerken over versleuteling van persoonsgegevens).

Bijzondere persoonsgegevens

De inzet van gezichtsherkenningstechnologie op de in dit rapport geschetste wijze betreft het gebruik van biometrische gegevens met het oog op de unieke identificatie van een persoon. Dat gebruik van biometrische gegevens kwalificeert, zoals reeds opgemerkt (zie paragraaf 4.1.3), als een verwerking van bijzondere persoonsgegevens. De inzet van gezichtsherkenningstechnologie is op grond van de AVG alleen toelaatbaar als een beroep kan worden gedaan op een uitzonderingsgrond.

De eventuele inzet van stemherkenningstechnologie ten behoeve van de identificatie van betrokkenen kwalificeert ook als de verwerking van biometrische gegevens met

het oog op de unieke identificatie van een persoon, en daarmee als bijzonder persoonsgegeven.

Wij staan in hoofdstuk 6 stil bij mogelijke uitzonderingsgronden voor de verwerking van biometrische gegevens.

Bij identificatie middels stoelnummerregistratie zal, anders dan bij de inzet van gezichtsherkenningstechnologie, in beginsel geen sprake zijn van de verwerking van bijzondere persoonsgegevens. Hoewel het zo is dat bij identificatie middels stoelnummerregistratie en de vastgelegde beelden uit die vastgelegde beelden ook informatie kan worden afgeleid over iemands religie, gezondheid, ras of etniciteit, hoeft daarbij niet steeds sprake te zijn van de verwerking van bijzondere persoonsgegevens. De verwerking van beelden betreft pas een verwerking van bijzondere persoonsgegevens op het moment dat de (indirecte) bijzondere persoonsgegevens worden geanalyseerd met als doel het (op basis van dat gegeven) identificeren van de desbetreffende persoon. Dat is bijvoorbeeld het geval als de camera's gericht zijn op identificatie, zoals bij camera's met gezichtsdetectie of gezichtsherkenningstechnologie. Zie daarover ook paragraaf 4.2.1.

Wij kunnen evenwel niet uitsluiten dat een rechter of de AP daar anders tegenaan kijkt, mede in het licht van de ruimte voor interpretatie die de beleidsregels van de AP bevat. Gelet daarop bespreken wij in hoofdstuk 6 mogelijke doorbrekingsgronden.

Strafrechtelijke persoonsgegevens

Ook hier geldt dat niet kan worden uitgesloten dat bij de inzet van slimme technologie beelden worden geanalyseerd die een zwaardere verdenking dan een redelijk vermoeden van schuld kunnen dragen. Aangezien in zoverre niet kan worden uitgesloten dat strafrechtelijke persoonsgegevens worden verwerkt, dient de voetbalclub te beschikken over een expliciete grondslag als bedoeld in artikel 10 AVG, respectievelijk de artikelen 31 − 33 UAVG.

4.2.3 Fase 3 − Gebruik van de gegevens ten behoeve van sanctieoplegging

Persoonsgegevens

In deze fase komen de persoonsgegevens uit fase 1 (over het gesignaleerde incident) en uit fase 2 (over de identiteit van de daarbij betrokken personen) samen ten behoeve van het opleggen van een sanctie. Dat zijn, als gezegd, persoonsgegevens waarop de AVG van toepassing is.

Bijzondere persoonsgegevens

In het geval gebruik wordt gemaakt van de beschreven gezicht- en/of van stemherkenningstechnologie zullen de persoonsgegevens die in deze fase worden verwerkt (deels) ook bijzondere persoonsgegevens kunnen betreffen.

Daarnaast is in deze fase mogelijk sprake van de verwerking van andere bijzondere persoonsgegevens, te weten van de beelden die rasgegevens bevatten die (onvermijdelijk) worden verwerkt voor de identificatie van de persoon (zie daarover paragraaf 4.2.2 hierboven).

Strafrechtelijke persoonsgegevens

Ook hier geldt dat niet kan worden uitgesloten dat bij de inzet van slimme technologie beelden worden geanalyseerd die een zwaardere verdenking dan een redelijk vermoeden van schuld kunnen dragen. Aangezien in zoverre niet kan worden uitgesloten dat strafrechtelijke persoonsgegevens worden verwerkt, dient de voetbalclub te beschikken over een expliciete grondslag als bedoeld in artikel 10 AVG, respectievelijk de artikelen 31 − 33 UAVG.

4.2.4 Tot slot: toepasselijkheid Wpg en Wjsg

Bij het voorgaande zijn wij ervan uitgegaan dat de slimme technologie voor de signalering van incidenten (fase 1) zal worden ingezet door de BVO's, nu zij primair verantwoordelijk zijn voor het ordentelijk verloop van voetbalwedstrijden en in dat kader ook op dit moment al verplicht zijn videocamera's in te zetten tijdens wedstrijden (zie daarover paragraaf 3.2 en hierna hoofdstuk 5).

Evenwel is tijdens een wedstrijd veelal ook iemand van de politie in de commandoruimte aanwezig. Deze medewerker zal op dat moment mogelijkerwijs ook de opnames kunnen raadplegen die op dat moment worden gemaakt en op beeldschermen worden afgespeeld. Hoewel de opnames niet worden gemaakt ten behoeve van de politietaak, raadpleegt (verwerkt) de politiemedewerker op dat moment wel de opnames in zijn hoedanigheid als politiemedewerker en daarmee bij het uitvoeren van zijn politietaak. In zoverre zouden de persoonsgegevens die de politieambtenaar voor eigen gebruik overneemt en verwerkt ook als politiegegevens kunnen kwalificeren. Direct gevolg daarvan is dat de Wpg van toepassing is.

Ook in de identificatiefase (fase 2) gaan wij ervan uit dat de registratiestap wordt uitgevoerd door de BVO's, en dat de politie en/of het OM daar op voorhand geen toegang toe heeft dan wel anderszins betrokkenheid bij heeft. De Wpg en/of de Wjsg is op de verwerking van persoonsgegevens bij de registratie dan niet van toepassing.

Voor de vraag of dat in de vergelijkingsstap anders is, is bepalend of de politie en/of het OM bij die vergelijkingsstap betrokken is. Op dit moment is nog niet duidelijk

welke partij de biometrische vergelijking gaat maken. Dat zou de BVO kunnen zijn op het moment dat zich een voorval heeft voorgedaan, of de KNVB op het moment dat melding wordt gemaakt van een incident via de KVV. Op de daarmee gepaard gaande verwerkingen zou in beide gevallen de AVG van toepassing zijn. Is het echter de politie en/of het OM die het betreffende beeldmateriaal met het referentiemateriaal gaat vergelijken, dan kan de Wpg respectievelijk Wjsg van toepassing zijn in plaats van de AVG.

Tot slot geldt voor de sanctiefase (fase 3) dat zodra politie en/of het OM overgaan tot opsporing of vervolging – en in dat kader persoonsgegevens verwerken - de Wpg respectievelijk Wjsg op hen van toepassing is in plaats van de AVG.

5 WIE VERWERKEN PERSOONSGEGEVENS?

In het vorige hoofdstuk is vastgesteld dat bij inzet van slimme technologie in voetbalstadions persoonsgegevens worden verwerkt en de AVG daarop van toepassing is. Vervolgens is de vraag wie deze persoonsgegevens verwerken. Dat is relevant om te bepalen wie de verwerkingsverantwoordelijken en eventuele (sub)verwerkers zijn, en daarmee op wie de verschillende verplichtingen rusten die uit de AVG volgen.

5.1 Juridisch kader

5.1.1 De verwerkingsverantwoordelijke

Een verwerkingsverantwoordelijke is degene die, alleen of samen met anderen, het doel en de middelen van de verwerking van persoonsgegevens vaststelt.[52]

> Met het bepalen van het doel van de verwerking wordt bedoeld dat de verwerkingsverantwoordelijke de zeggenschap heeft over waarom de persoonsgegevens worden verwerkt en voor welke concrete doelen de persoonsgegevens zullen worden ingezet. Het vaststellen van het doel van de verwerking is een exclusieve bevoegdheid van de verwerkingsverantwoordelijke.
>
> Met het vaststellen van de middelen van de verwerking wordt gedoeld op het vaststellen van de wijze waarop de verwerking plaats zal vinden, kortom: hoe worden de persoonsgegevens verwerkt ten behoeve van het vastgestelde doel.

Het is mogelijk dat in de bijzondere wetten uitdrukkelijk is bepaald wie verwerkingsverantwoordelijke is voor de persoonsgegevens die op grond van de betreffende wet mogen worden verwerkt.

5.1.2 Gezamenlijke verwerkingsverantwoordelijken

Indien twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en de middelen van de verwerking bepalen, wordt op grond van de AVG gesproken van 'gezamenlijke verwerkingsverantwoordelijken'.[53] De nationale en Europese rechtspraak bieden nadere handvatten wanneer daadwerkelijk kan worden gesproken van (gezamenlijke) verwerkingsverantwoordelijkheid. Het begrip verwerkingsverantwoordelijke wordt in de rechtspraak van het Europese Hof van Justitie ruim uitgelegd. Doel van deze ruime uitleg is het bieden van een doeltreffende en volledige bescherming van betrokkenen.[54] Het Hof acht het voor de kwalificatie van gezamenlijke verwerkingsverantwoordelijke niet noodzakelijk dat de betreffende

[52] Artikel 4, aanhef en onder 7, AVG.
[53] Artikel, 26, eerste lid, AVG.
[54] Zie HvJ EU 13 mei 2014, ECLI:EU:C:2014:317 (Google Spain), par. 34 en HvJ EU 5 juni 2018, ECLI:EU:C:2018:388 (Wirtschaftsakademie), par 28.

rechtspersoon toegang heeft tot de persoonsgegevens.[55] Evenmin hoeft te worden aangetoond dat de betreffende rechtspersoon richtsnoeren of instructies voor die verwerking heeft gegeven aan de andere rechtspersoon over de verwerking van persoonsgegevens. Van een gezamenlijke verwerkingsverantwoordelijkheid kan al sprake zijn in het geval een rechtspersoon het doel van het verzamelen en het verder verwerken van de persoonsgegevens vaststelt en (ten behoeve van het vastgestelde doel) activiteiten organiseert, coördineert of aanmoedigt in het kader waarvan de rechtspersoon ten behoeve van een derde persoonsgegevens verwerkt. In een dergelijk geval neemt de rechtspersoon deel aan het vaststellen van het doel en de middelen van de verwerking.[56]

Het bestaan van een gezamenlijke verantwoordelijkheid uit zich overigens niet noodzakelijkerwijs in een gelijkwaardige verantwoordelijkheid voor één en dezelfde verwerking van persoonsgegevens. Bij een gezamenlijke verantwoordelijkheid kunnen de partijen in verschillende mate betrokken zijn bij de gezamenlijke vaststelling en hoeft hun inbreng niet even groot te zijn.[57]

Indien sprake is van een gezamenlijke verwerkingsverantwoordelijkheid zullen de verwerkingsverantwoordelijken een zogenoemde onderlinge regeling moeten vaststellen. De onderlinge regeling dient in te gaan op, kort gezegd, hoe de gezamenlijke verwerkingsverantwoordelijken ervoor zullen zorgen dat aan de AVG wordt voldaan, in het bijzonder waar het de uitoefening van de rechten van de betrokkenen en de informatieverplichting betreft. De regeling moet aan de betrokkenen beschikbaar worden gesteld.

CONFIDENTIAL

5.1.3 (Sub)verwerkers

Indien de verwerkingsverantwoordelijken bij de inzet van slimme technologie gebruik maken van een verwerker, dient door middel van (onder meer) een verwerkersovereenkomst te worden geborgd dat de vereisten van de AVG strikt worden nageleefd.

De verwerker is degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.[58] De verwerker ontleent zijn bevoegdheid om persoonsgegevens te verwerken aan de bevoegdheid van de verwerkingsverantwoordelijke die hem inschakelt. De bevoegdheden van een verwerker moeten zijn vastgelegd in een verwerkersovereenkomst.[59]

Kenmerkend voor een verwerker is dat de verwerker:

---

55 Zie de arresten van 5 juni 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, punt 38, en 10 juli 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, punt 69).
56 Zie HvJ EU 10 juli 2018, ECLI:EU:C:2018:551 (Finland t. Jehovan todistajat), par. 71 – 74.
57 Zie Artikel 29-Werkgroep, 'Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker'', p. 22.
58 Artikel 4, aanhef en onder 8, AVG.
59 Artikel 28, derde lid, AVG.

- een externe natuurlijke persoon, rechtspersoon, overheidsinstantie, dienst of orgaan is, die geen onderdeel vormt van de verwerkingsverantwoordelijke, en;
- persoonsgegevens voor de verwerkingsverantwoordelijke verwerkt − en dus niet voor zichzelf.[60]

Voor de kwalificatie van verwerker is bepalend of de partij aanwijzingen van de verwerkingsverantwoordelijke dient op te volgen met betrekking tot de verwerking van persoonsgegevens. Zo ja, dan is de partij een verwerker. Uitgangspunt is dat de verwerker niet mag afwijken van de afspraken die in de verwerkersovereenkomst met de verwerkingsverantwoordelijke zijn gemaakt. Dat betekent overigens niet dat de verwerker op detailniveau aanwijzingen van de verwerkingsverantwoordelijke moet ontvangen en volgen over de gegevensverwerking, maar (in ieder geval) wel voor zover het gaat om het doel van de verwerking en de wezenlijke aspecten van de middelen voor de verwerking.[61]

5.2 Kwalificatie van de betrokken partijen

Op dit moment is niet (precies) duidelijk welke partijen in de verschillende fases betrokken zullen zijn bij de inzet van slimme technologie in voetbalstations. Het is daarom in dit stadium nog niet eenduidig vast te stellen wie verantwoordelijk zal zijn voor welke verwerking. Wel kunnen op basis van de stand van zaken op dit moment een aantal uitgangspunten worden geformuleerd. Die bespreken wij hieronder per fase.

Op dit moment is ook nog niet duidelijk welke partij(en) de slimme technologie zullen leveren en beheren. Voorstelbaar is dat dergelijke partijen, als bij het leveren en/of beheren van de technologie persoonsgegevens worden verwerkt, kwalificeren als verwerker van de hierna genoemde verwerkingsverantwoordelijken. Mochten deze partijen de persoonsgegevens (ook) voor zichzelf verwerken, dan kwalificeren zij voor dat deel zelf ook als verwerkingsverantwoordelijke. Dit vergt een nadere beoordeling.

5.2.1 Fase 1 − Signaleren van discriminatie en racisme

- De BVO's zullen naar alle waarschijnlijkheid kwalificeren als verwerkingsverantwoordelijke voor de inzet van slimme technologie in de signaleringsfase. Dat is in lijn met de huidige inzet van videocamera's in voetbalstadions, waarbij de BVO's primair verantwoordelijk zijn voor het ordentelijk verloop van de wedstrijden en in dat kader videocamera's inzetten in het stadion.

---

[60] Op het moment dat een verwerker verwerkingen voor zichzelf (of in strijd met de instructies van de verwerkingsverantwoordelijke) verricht, en aldus feitelijk handelt als verwerkingsverantwoordelijke, zal de verwerker (voor dat deel) worden aangemerkt als verwerkingsverantwoordelijke.

[61] Zie Artikel 29-Werkgroep, 'Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"', 16 februari 2010, p. 29.

- De KNVB kwalificeert mogelijk (ook) als verwerkingsverantwoordelijke in de signaleringsfase. Of dat het geval is, hangt af van de mate waarin de KNVB de BVO's verplicht slimme technologie in te zetten en de wijze waarop dat dient te geschieden, bijvoorbeeld in de (licentie-)eisen. Goed voorstelbaar is dat in dat geval de BVO's en de KNVB kwalificeren als gezamenlijke verwerkingsverantwoordelijken.

- Indien politie en/of het OM ook zeggenschap zou krijgen over de wijze waarop en/of de doeleinden waarvoor de slimme technologie in de signaleringsfase wordt ingezet, zouden zij eveneens als verwerkingsverantwoordelijke(n) kunnen kwalificeren. Op dit moment hebben wij geen aanwijzingen dat politie en/of het OM inspraak krijgt in de wijze waarop en de doeleinden waarvoor de slimme technologie in de signaleringsfase wordt ingezet.

5.2.2 Fase 2 – Identificeren van de betrokkene

Gezichtsherkenningstechnologie

- Het is waarschijnlijk dat het referentiemateriaal wordt verkregen door de BVO's. De BVO's kwalificeren in dat geval als verwerkingsverantwoordelijke voor de daarmee gepaard gaande verwerkingen.

- De BVO's kunnen ook verwerkingsverantwoordelijke zijn voor de biometrische vergelijking tussen het referentiemateriaal en de opnames van een incident, een en ander afhankelijk van de partij die deze vergelijking gaat uitvoeren.

- De KNVB kan verwerkingsverantwoordelijke zijn voor de registratie- en vergelijkingsstappen in de identificatiefase voor zover zij zeggenschap heeft over de wijze waarop de BVO's gezichtsherkenningstechnologie moeten gaan inzetten in de voetbalstadions, bijvoorbeeld in de (licentie-)eisen. Goed voorstelbaar is dat in dat geval de BVO's en de KNVB kwalificeren als gezamenlijke verwerkingsverantwoordelijken.

- Politie en/of het OM kunnen ook als verwerkingsverantwoordelijke(n) kwalificeren indien zij betrokkenheid hebben bij de identificatie door middel van biometrische gegevens.

Stoelnummerregistratie

- Wij gaan ervan uit dat de stoelnummerregistratie en daarbij aan te leveren persoonsgegevens primair onder de verantwoordelijkheid van de BVO's vallen, en zij daarvoor kwalificeren als de verwerkingsverantwoordelijken.

- De KNVB kan ook als verwerkingsverantwoordelijke kwalificeren. Of dat het geval is, hangt af van de mate waarin de KNVB de BVO's verplicht stoelnummerregistratie in te voeren en zeggenschap heeft over de wijze waarop dat dient te geschieden, bijvoorbeeld in de (licentie-)eisen. Goed voorstelbaar is dat in dat geval de BVO's en de KNVB in dat geval kwalificeren als gezamenlijke verwerkingsverantwoordelijken.

- Politie en/of het OM kunnen ook als verwerkingsverantwoordelijke(n) kwalificeren indien zij betrokkenheid hebben bij de identificatie door middel van stoelnummerregistratie.

5.2.3 Fase 3 – Gebruik van de gegevens ten behoeve van sanctieoplegging

- De BVO's kwalificeren als verwerkingsverantwoordelijke voor de invoer van de persoonsgegevens in de KVV. Ook zijn zij verwerkingsverantwoordelijke voor de persoonsgegevens die zij verwerken wanneer zij overgaan tot het opleggen van een lokaal stadionverbod.

- De KNVB is verwerkingsverantwoordelijke voor de persoonsgegevens die zij ontvangt middels de KVV en (verder) verwerkt met het oog op het opleggen van een landelijk stadionverbod. Wij gaan ervan uit dat de BVO's en de KNVB gezamenlijke verwerkingsverantwoordelijken zijn voor de persoonsgegevens die middels de KVV worden verwerkt.

- De korpschef van de politie[62] is verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens met het oog op de goede uitvoering van politietaken. Het gaat dan zowel om de verwerking van persoonsgegevens ten behoeve van de handhaving van de openbare orde rondom wedstrijden, als om de verwerking van persoonsgegevens met het oog op de opsporing van strafbare feiten (bijvoorbeeld nadat aangifte is gedaan).

- Het OM[63] is verwerkingsverantwoordelijke voor de persoonsgegevens die het verwerkt in het kader van de vervolging van strafbare feiten.

[62] Zie artikel 1, aanhef en onder f, sub 1, Wpg.
[63] Zie over de verwerking van justitiële gegevens, strafvorderlijke gegevens, tenuitvoerleggingsgegevens en gerechtelijke strafgegevens artikel 1, aanhef en onder k, Wjsg.

6 GRONDSLAGEN, NOODZAKELIJKHEID EN DOELBINDING

Zoals vastgesteld in paragraaf 4.2 van dit rapport, worden er bij de inzet van slimme technologieën persoonsgegevens verwerkt van toeschouwers. Het kan daarbij (onder meer) gaan om het (enkel) verwerken van beelden en geluid, maar ook om het toepassen van algoritmes en gezichtsherkenning. Op grond van artikel 6, eerste lid, van de AVG mag de verwerking van persoonsgegevens alleen plaatsvinden voor zover daarvoor een toereikende wettelijke grondslag bestaat. Van belang daarbij is dat de aard en de omvang van de gegevensverwerking die met de toepassing van slimme technologieën gepaard gaat, is beperkt tot het strikt noodzakelijke. Dit betreft het zogenoemde 'noodzakelijkheidsbeginsel' (artikel 5, eerste lid, aanhef en onder c, AVG). Tot slot geldt als uitgangspunt dat het verstrekken van de door de camera's vastgelegde geluiden en beelden (en daarmee de persoonsgegevens van toeschouwers) door de BVO plaatsvindt, en verstrekking daarvan aan (bijvoorbeeld) de KNVB en/of de politie plaatsvindt ten behoeve van een nieuw doel (namelijk ten behoeve van daadwerkelijke sanctieoplegging). Een dergelijke 'verdere verwerking' dient ofwel verenigbaar te zijn met het oorspronkelijk doel waarvoor de BVO de persoonsgegevens heeft verzameld, ofwel, als sprake is van een onverenigbare verdere verwerking, op een aparte wettelijke grondslag te kunnen worden gebaseerd (als bedoeld in artikel 6, vierde lid, AVG).

In dit hoofdstuk analyseren wij of, en zo ja, in hoeverre de in hoofdstuk 5 genoemde (mogelijke) verwerkingsverantwoordelijken bij de inzet van slimme technologieën voldoen aan deze juridische voorwaarden.

6.1 Juridisch kader

6.1.1 Wettelijke grondslag

Het staat vast dat met het maken van camerabeelden (eventueel) in combinatie met de inzet van slimme technologieën, persoonsgegevens van de toeschouwers worden verwerkt. De in hoofdstuk 5 genoemde verwerkingsverantwoordelijken dienen als gezegd te beschikken over een wettelijke grondslag als bedoeld in artikel 6, eerste lid, AVG.[64]

Artikel 6, eerste lid, van de AVG bepaalt dat een verwerking van persoonsgegevens is toegestaan voor zover daarvoor een zogenoemde 'wettelijke grondslag' bestaat. De algemene wettelijke grondslagen van artikel 6 AVG luiden als volgt:

> a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;

[64] Een afzonderlijke grondslag is overigens niet vereist indien sprake is van een verenigbare verdere verwerking als bedoeld in artikel 6, vierde lid, AVG. Zie daarover uitgebreider paragraaf 6.1.3 van dit rapport.

b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;

c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;

f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Gerechtvaardigd belang (artikel 6, eerste lid, aanhef en onder f, AVG)

Voor dit rapport is met name artikel 6, eerste lid, aanhef en onder f, AVG (de verwerking is noodzakelijk voor een zwaarwegend gerechtvaardigd belang) relevant. De betrokken verwerkingsverantwoordelijke kan zich op deze wettelijke grondslag beroepen voor zover wordt voldaan aan de volgende criteria:

- Allereerst moet sprake zijn van een echt, concreet, rechtstreeks 'gerechtvaardigd belang' van de verwerkingsverantwoordelijke (bijv. de BVO) of een derde (bijv. de supporter van de tegenstander die het mikpunt is van de discriminerende of racistische uitlatingen). De AP ziet onder meer het borgen van een veilig leven in een dreigende situatie, het tegen gaan van inbreuken op persoonlijkheidsrechten, het tegengaan van onrechtmatig gedrag en het nakomen van zorgplichten ten aanzien van klanten als gerechtvaardigde belangen.
- De verwerking moet strikt noodzakelijk zijn om het gerechtvaardigde belang te behartigen.
- Tot slot dient een afweging plaats te vinden tussen de belangen van de BVO (en/of diens partners) enerzijds en de belangen van de betrokkenen anderzijds. De gerechtvaardigde belangen dienen zwaarder te wegen dan de belangen van de betrokkenen. De volgende factoren zijn bij deze afweging relevant:[65]
  - de gevolgen voor de betrokkene;
  - de (aanvullende) waarborgen die de verwerkingsverantwoordelijke of derde heeft getroffen om ongewenste gevolgen voor de betrokkene te voorkomen of beperken;

[65] WP29, Advies 06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG, vastgesteld op 9 april 2014, par. III.3.4.

- de ernst van de inmenging op het grondrecht van de betrokkene;
- of de betrokkene de verwerking min of meer kan verwachten, bijvoorbeeld als vervolg op een eerdere verwerking waarvoor diegene toestemming heeft gegeven of als vervolg op verwerkingen die noodzakelijk zijn om een contract uit te voeren.

Van belang is tot slot dat overheidsinstanties bij de uitoefening van hun publieke taken nooit een verwerking van persoonsgegevens mogen baseren op de gerechtvaardigd belang grondslag. Zij dienen een dergelijke verwerking te baseren op artikel 6, eerste lid, aanhef en onder e, AVG (de verwerking is noodzakelijk voor de uitvoering van de publiekrechtelijke taak).

Noodzakelijk voor de uitvoering van de overeenkomst (artikel 6, eerste lid, aanhef en onder b, AVG).

Persoonsgegevens mogen daarnaast worden verwerkt indien de verwerking noodzakelijk is voor de uitvoering van een overeenkomst of het treffen van precontractuele maatregelen (artikel 6, eerste lid, aanhef en onder b, AVG). Een beroep op deze wettelijke grondslag is alleen mogelijk indien de betrokkene partij is bij de overeenkomst of als de betrokkene heeft verzocht om het treffen van precontractuele maatregelen. De overeenkomst in dit concrete geval is de aankoop van het toegangsbewijs door de toeschouwers. Daarmee committeert de toeschouwer zich (automatisch) aan de huisregels van de BVO en de algemene voorwaarden die door de KNVB zijn geformuleerd, waaronder het maken van beeld- en geluidsopnamen (artikel 9 van de Algemene Voorwaarden)[66] en het verbod om zich onrechtmatig in het stadion te gedragen (artikel 8.5 van de Algemene Voorwaarden). Het is twijfelachtig of de inzet van slimme technologieën daadwerkelijk zou kunnen worden aangemerkt als strikt noodzakelijk voor de uitvoering van de overeenkomst. De inzet van slimme technologieën volgt veel meer uit het gerechtvaardigde belang van de BVO om discriminatie en racisme te signaleren, identificeren en aan te pakken. Tegen deze achtergrond ligt het meer voor de hand de verwerking van persoonsgegevens te baseren op de hiervoor genoemde f-grond.

Toestemming (artikel 6, eerste lid, aanhef en onder a, AVG).

Een (in de praktijk geregeld) door de BVO ingeroepen wettelijke grondslag bij de verkoop van voetbalkaartjes betreft het vragen van toestemming voor (onder meer) het filmen van toeschouwers en de daarmee gepaarde verwerking van diens persoonsgegevens. Van rechtsgeldige toestemming in de zin van de AVG is sprake indien de toestemming van de betrokkene (i) vrijelijk, (ii) specifiek, (iii) geïnformeerd en (iv) op een ondubbelzinnige wijze is verkregen.

i. Vrijelijk

De eerste voorwaarde, (i) *vrijelijke* toestemming, houdt in dat de betrokkene

[66] https://www.knvb.nl/downloads/bestand/2785/knvb-standaardvoorwaarden-per-1-september-2014

daadwerkelijk een vrije keuze moet hebben of hij toestemming geeft voor de verwerking van zijn persoonsgegevens. Een belangrijke eis daarbij is dat de betrokkene geen nadelige gevolgen ondervindt indien hij zijn toestemming weigert of intrekt.[67] Voorts is van belang dat de toestemming *apart* moet worden gevraagd. Het verzoek om toestemming mag niet zijn verstopt in bijvoorbeeld de algemene voorwaarden of een contract. Het verzoek om toestemming voor de verwerking van persoonsgegevens moet duidelijk te onderscheiden zijn.[68]

Onzeker is of er in deze situatie kan worden gesproken van vrije toestemming van de toeschouwers. Om tot het stadion toegang te krijgen is toestemming vereist. Er kan derhalve worden gezegd dat het weigeren van de toestemming een nadelig gevolg heeft voor de toeschouwer − hij komt het stadion niet in. En dat brengt met zich mee dat het onzeker is of kan worden gezegd dat deze toestemming in vrijheid is gegeven.

ii. Specifiek

De tweede voorwaarde voor het verkrijgen van rechtsgeldige toestemming is dat de toestemming gespecificeerd moet zijn: er moet om specifieke, gerichte toestemming worden gevraagd. Het toestemmingsformulier moet zo zijn vormgegeven dat de betrokkene zijn toestemming per verwerkingsverantwoordelijke, per doel en per type persoonsgegevens kan differentiëren.[69] De doeleinden mogen niet zodanig vaag zijn dat zij na het verkrijgen van toestemming ruimer zouden kunnen worden geïnterpreteerd.

iii. Geïnformeerd

De derde voorwaarde voor het verkrijgen van rechtsgeldige toestemming is dat sprake moet zijn van *geïnformeerde* toestemming. De betrokkene dient voorafgaand aan het verlenen van zijn toestemming uitvoerig te zijn geïnformeerd over de beoogde verwerking (met slimme technologieën), zodat hij een geïnformeerde beslissing kan nemen of hij al dan niet zijn toestemming verleent.

De AVG schrijft niet voor op welke wijze de hiervoor genoemde informatie moet worden gegeven. De wijze waarop om toestemming wordt gevraagd is in zoverre vormvrij. Dat neemt niet weg dat bepaalde kwaliteitseisen gelden ten aanzien van de inhoud van de informatie. Zo moet het verzoek om toestemming in een begrijpelijke en gemakkelijke toegankelijke vorm en in duidelijke en eenvoudige taal worden gepresenteerd.[70]

iv. 'Ondubbelzinnig'

De laatste voorwaarde voor het verkrijgen van rechtsgeldige toestemming is dat de toestemming ondubbelzinnig − door middel van een actieve handeling − moet zijn

---

67 Vgl. Overwegingen 42 AVG: "Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen." Zie tevens: Artikel-29 Werkgroep, 'Guidelines on consent under Regulation 2016/679' van 10 april 2018, WP259 rev. 01, p. 5-6.

68 Vgl. Artikel 7, vierde lid, AVG jo. overweging 43 AVG.

69 Daarbij kan gebruik worden gemaakt van afzonderlijke (digitale) formulieren per betrokkene.

70 Artikel 7, tweede lid, AVG.

geuit. Er dient kortom altijd sprake te zijn van een 'opt-in'. De wijze waarop dit moet gebeuren, is in principe vormvrij. Het actief kunnen aankruisen van een vakje is in de ogen van de Europese privacy toezichthouders voldoende. Een al aangevinkt vakje dat kan worden uitgezet (een 'opt-out') is niet voldoende.

Aanvullende voorwaarden

Voor zover 'uitdrukkelijke toestemming' rechtsgeldig kan worden verkregen, geldt als aanvullende voorwaarden dat:

- de verwerkingsverantwoordelijke kan aantonen wanneer en op welke wijze hij toestemming van de betrokkene heeft verkregen voor het verwerken van de persoonsgegevens, bijvoorbeeld door middel van het bijhouden van een 'toestemmingenregister'[71];
- de betrokkene de mogelijkheid moet krijgen om zijn toestemming gemakkelijk weer in te trekken.

Aangezien voor de KNVB en de BVO alleen artikel 6, eerste lid, aanhef en onder f, AVG een grondslag lijkt te bieden voor de inzet van slimme technologieën zullen wij in het verdere vervolg van dit rapport ons tot deze wettelijke grondslagen beperken.

6.1.2 Noodzakelijkheidsbeginsel

Het door middel van de inzet van slimme technologieën verwerken van persoonsgegevens ten behoeve van de signalering, identificering en aanpak van racisme en discriminatie door toeschouwers, moet voldoen aan het noodzakelijkheidsbeginsel van artikel 5, eerste lid, aanhef en onder c, AVG, ook wel aangeduid als 'het beginsel van dataminimalisatie'.

Het noodzakelijkheidsbeginsel heeft gevolgen voor de toegang tot, de omvang van en de aard van de persoonsgegevens die door middel van de inzet van slimme technologieën door de BVO's en diens partners mogen worden verwerkt. De persoonsgegevens dienen toereikend en ter zake dienend te zijn en moeten beperkt blijven tot het strikt noodzakelijke. Kort en goed houdt dit in dat de voetbalclub en diens partners enkel '*need tot know'*-informatie mag verwerken, in plaats van '*nice to know'*-informatie.

Uit het noodzakelijkheidsbeginsel volgt voorts dat de privacyinbreuk die met de inzet van de slimme technologie gepaard gaat in evenredige verhouding moet staan tot het doel waarvoor deze technologie wordt ingezet, te weten het signaleren, identificeren en aanpakken van racisme of discriminatie door voetbalsupporters. Daarnaast mogen de BVO en de overige in hoofdstuk 5 genoemde verwerkingsverantwoordelijken, slechts overgaan tot het verwerken van persoonsgegevens door middel van slimme

[71] Uit dit toestemmingenregister zou moeten blijken (i) hoe toestemming is verkregen, (ii) wanneer en waarvoor de toestemming is verleend en (iii) de informatie die ten tijde van het verkrijgen van de toestemming door de verwerkingsverantwoordelijke is verstrekt.

technologieën indien het hiervoor beschreven doel niet met minder vergaande maatregelen kan worden bereikt (‘subsidiariteit’).

Het noodzakelijkheidsbeginsel zal ook technisch moeten worden geborgd, zodat kan worden voldaan aan de beginselen van privacy by design & default. Op grond van privacy by design & default zal de BVO en andere betrokken partijen, waar mogelijk technisch moeten borgen dat het noodzakelijkheidsbeginsel door ontwerp en standaardinstellingen gewaarborgd blijft. De voetbalclub en de andere in hoofdstuk 5 genoemde verwerkingsverantwoordelijken dienen in iedere fase kritisch te bezien welke privacyverhogende maatregelen getroffen kunnen worden.

Het naleven van privacy by design & default betreft een zeer algemene verplichting, waarbij de voetbalclub en diens partners aan de hand van verschillende factoren een belangenafweging moeten maken ten aanzien van de technische en organisatorische aspecten van de met de gekozen (slimme) technologie gepaarde gegevensverwerking. Die factoren zijn (onder meer) de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context en het doel van de verwerking en de risico’s (waarschijnlijkheid en ernst[72]) voor de rechten en vrijheden van de betrokkenen. Deze beoordeling vindt plaats voorafgaand aan het gebruik van de (nieuwe) technologie en kan invloed hebben op de inrichting daarvan. Met inachtneming van die factoren zal de voetbalclub en diens partners bij het ontwerp van de slimme technologie passende technische en organisatorische maatregelen moeten treffen. Het doel daarvan is dat de gegevensbeschermingsbeginselen − zoals dataminimalisatie − op een doeltreffende manier worden toegepast en in het technische ontwerp en ontwikkelingsproces de nodige waarborgen worden ingebouwd ter naleving van de voorschriften van de AVG en ter bescherming van de rechten van de betrokkenen (artikel 25, eerste lid, AVG).

De verplichting van privacy by design & default is het best te begrijpen als een zorgplicht van de voetbalclub en (eventueel) diens partners om een zo beperkt mogelijke inbreuk op de persoonlijke levenssfeer te maken bij de verwerking van persoonsgegevens. Deze zorgplicht zal in verschillende contexten geconcretiseerd moeten worden, maar verschillende elementen worden al expliciet in de (toelichting bij[73]) de AVG genoemd: het minimaliseren van de verwerking van persoonsgegevens, het zo spoedig mogelijk pseudonimiseren van persoonsgegevens, het voor de betrokkene transparant maken van de functies en de verwerking van persoonsgegevens, het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking en het in staat stellen van de verwerkingsverantwoordelijke om beveiligingskenmerken te creëren en te verbeteren.

Ook dient de voetbalclub passende technische en organisatorische maatregelen te treffen om ervoor te zorgen dat slechts persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt ten

[72] Zie voor een concretisering hiervan de overwegingen 75 en 76 van de AVG.
[73] Zie overweging 78 van de considerans van de AVG.

aanzien van:

- de hoeveelheid verzamelde persoonsgegevens (zo min mogelijk);
- de mate waarin zij worden verwerkt (hoe minder vaak, hoe beter);
- de termijn waarvoor zij worden opgeslagen (hoe korter, hoe beter), en;
- de toegankelijkheid ervan (hoe minder mensen toegang hebben, hoe beter).

6.1.3 Doelbinding en verdere verwerkingen

Voor de 'verdere verwerking' van beelden en geluidsopnamen (in dit concrete geval de verstrekking door de BVO aan derden via de KVV) dient een aparte wettelijke grondslag als bedoeld in artikel 6, vierde lid, AVG te bestaan.

Een verdere verwerking mag ingevolge artikel 6, vierde lid, AVG slechts plaatsvinden voor zover de verwerking berust op (i) toestemming, (ii) een Europese of nationale wettelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van een in artikel 23, eerste lid, AVG bedoelde doelstelling óf (iii) het doeleinde van de verdere verwerking verenigbaar is met het oorspronkelijke doel van de verwerking van de gegevens. Of en zo ja, in hoeverre sprake is van een verenigbare verdere verwerking wordt getoetst aan de hand van de volgende criteria:

- Het verband tussen de doeleinden waarvoor de gegevens zijn verzameld en de doeleinden van de verdere verwerking;
- Het kader waarin de persoonsgegevens zijn verzameld en dan met name de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke (ook wel: de wijze van verkrijging en de verwachting van de betrokkene);
- De aard van de gegevens;
- De mogelijke gevolgen van de voorgenomen verdere verwerking voor betrokkenen; en
- Het bestaan van passende waarborgen, zoals pseudonimisering.

Indien sprake is van een verenigbare verdere verwerking, dan is bij een *interne* verdere verwerking (door dezelfde verwerkingsverantwoordelijke, bijvoorbeeld de voetbalclub) geen afzonderlijke wettelijke grondslag als bedoeld in artikel 6, eerste lid, AVG vereist. Gaat het bij de verdere verwerking om een (externe) verstrekking aan een andere verwerkingsverantwoordelijke, dan moet die andere verwerkingsverantwoordelijke vanzelfsprekend wel een eigen grondslag hebben om de ontvangen gegevens te verwerken.

> Zie *Kamerstukken II* 2018/19, 34 851, nr. 3, p. 38.[74]

[74] Deze opmerking in de memorie van toelichting is toegevoegd naar aanleiding van het wetgevingsadvies van de Afdeling advisering van de Raad van State (Kamerstukken II 2017/18, 34 851, nr. 4, p. 36-38).

6.1.4 Uitzonderingsgronden voor bijzondere persoonsgegevens, waaronder biometrie

In hoofdstuk 4 is toegelicht dat de inzet van slimme technologieën in de signaleringsfase op zichzelf genomen niet lijkt te leiden tot het verwerken van bijzondere persoonsgegevens inzake (o.a.) ras of etnische afkomst, maar het wel mogelijk is dat bij bepaalde slimme technologieën in de identificatiefase biometrische persoonsgegevens zullen worden verwerkt. Voor het verwerken van biometrische gegevens met het oog op de unieke identificatie van een persoon geldt een verwerkingsverbod (artikel 9, eerste lid, AVG), tenzij dit verbod door middel van een expliciete wettelijke grondslag – een zogenoemde 'doorbrekingsgrond' of 'uitzonderingsgrond' – wordt doorbroken.

De algemene uitzonderingsgronden op het verbod om bijzondere persoonsgegevens te verwerken, staan beschreven in artikel 9 AVG en de artikelen 22 tot en met 33 van de UAVG. Ook een bijzondere wet kan een doorbrekingsgrond voor het verwerken van bijzondere persoonsgegevens bevatten.

Voor het verbod op de verwerking van biometrische gegevens met het oog op de unieke identificatie van een persoon zijn de volgende uitzonderingsgronden relevant.

Uitdrukkelijke toestemming (artikel 9, tweede lid, aanhef en onder a, AVG jo. artikel 22, tweede lid, aanhef en onder a, UAVG).

Het verbod bijzondere persoonsgegevens te verwerken, waaronder biometrische gegevens, is niet van toepassing indien de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van de biometrische gegevens voor een of meer welbepaalde doelen.

Statistische doeleinden (artikel 9, tweede lid, aanhef en onder j, AVG jo. artikel 24 UAVG)

Artikel 89 AVG jo. artikel 9, tweede lid, aanhef en onder j, AVG jo. 24 UAVG vormen een wettelijke grondslag en doorbrekingsgrond voor het verwerken van persoonsgegevens, waaronder bijzonder persoonsgegevens ten behoeve van statistisch onderzoek: de zogenoemde statistische onderzoeksexceptie.[75] Onder een onderzoek met een statistisch doeleinde wordt verstaan:

> "het verzamelen en verwerken van persoonsgegevens die nodig zijn voor statistische onderzoeken en voor het produceren van statistische resultaten. Die statistische resultaten kunnen ook voor andere doeleinden worden gebruikt, onder meer voor wetenschappelijke onderzoeksdoeleinden. Het statistische oogmerk betekent dat het resultaat van de verwerking voor

[75] Artikel 89 AVG bepaalt dat ten behoeve van statistische onderzoeken persoonsgegevens kunnen worden verwerkt. Artikel 9, tweede lid, aanhef en onder j, AVG jo. artikel 24 UAVG bepaalt in aanvulling daarop dat onder strikte voorwaarden ook bijzondere persoonsgegevens mogen worden verwerkt.

> statistische doeleinden niet uit persoonsgegevens, maar uit geaggregeerde gegevens bestaat, en dat dit resultaat en de persoonsgegevens niet worden gebruikt als ondersteunend materiaal voor maatregelen of beslissingen die een bepaalde natuurlijke persoon betreffen."[76]

Het trainen en ontwikkelen van het algoritme dat racistisch of discriminatoir gedrag herkent, zal kwalificeren als een vorm van statistisch onderzoek. Ook statistische onderzoeken met commerciële doeleinden kunnen worden gebaseerd op artikel 89 AVG.[77] Zoals volgt uit artikel 5, eerste lid, aanhef en onder b, AVG vormt de verwerking van persoonsgegevens ten behoeve van (onder meer) wetenschappelijk of statistisch onderzoek een verenigbare verwerking. Om in de ontwikkelingsfase een geslaagd beroep te kunnen doen op de statistische onderzoeksexceptie dient de ontwikkeling en training aan de volgende vereisten te voldoen. De ontwikkelaar moet borgen dat:

(a) Niet méér persoonsgegevens verzameld en geanalyseerd worden dan noodzakelijk is voor het beoogde onderzoek.
(b) Het resultaat van de verwerking voor wetenschappelijke doeleinden niet zal bestaan uit persoonsgegevens, maar slechts uit geaggregeerde – niet meer tot natuurlijke personen herleidbare – gegevens.
(c) De geanalyseerde onderliggende persoonsgegevens en het resultaat van de analyse niet (als ondersteunend materiaal) gebruikt worden om maatregelen of beslissingen te nemen die een bepaalde natuurlijke persoon betreffen.
(d) Er technische en organisatorische maatregelen worden getroffen om het voorgaande te verzekeren (waaronder functionele scheiding, anonimisering en pseudonimisering, verwijdering persoonsgegevens na afloop van het onderzoek en geheimhouding).

Indien wordt voldaan aan bovengenoemde voorwaarden, mogen normale persoonsgegevens worden verwerkt. Voor de verwerking van bijzondere persoonsgegevens gelden aanvullende vereisten op grond van artikel 24 UAVG. Kort en goed is de verwerking van bijzondere persoonsgegevens slechts toegestaan indien wordt voldaan aan de volgende randvoorwaarden:

(a) Het onderzoek moet een algemeen belang dienen.
(b) De verwerking van de bijzondere persoonsgegegevens moet voor het statistisch onderzoek noodzakelijk zijn.
(c) Het vragen van uitdrukkelijke toestemming van de betrokkene blijkt onmogelijk of kost onevenredige inspanning.

---

[76] Overweging 162 van de AVG.
[77] *Kamerstukken II 1998/99 25892, nr. 13, p. 8: "Ja. Zolang het resultaat geen betrekking heeft op identificeerbare natuurlijke personen, is – ook al worden voor het verkrijgen van dat resultaat wel persoonsgegevens gebruikt – sprake van statistisch onderzoek. In dat geval is het soepeler regime van de wet van toepassing. Wij verwijzen naar artikel 9, tweede lid, van het wetsvoorstel. Dit sluit aan bij de huidige praktijk."*

(d) Bij de uitvoering van het statistisch onderzoek is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer niet onevenredig wordt geschaad.

De instelling, uitoefening of onderbouwing van een rechtsvordering (artikel 9, tweede lid, aanhef en onder f, AVG jo. artikel 22, tweede lid, aanhef en onder e, UAVG)

In artikel 22, aanhef en onder e, UAVG is bepaald dat bijzondere persoonsgegevens mogen worden verwerkt voor zover dat noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering. Daarbij geldt overigens wel dat de rechtsvordering of de procedure reeds moet zijn ingesteld. De enkele mogelijkheid dat een procedure zal worden gestart, is aldus onvoldoende.

Een zwaarwegend algemeen belang en biometrische gegevens (artikel 9, tweede lid, aanhef en onder g, AVG jo. artikel 29 UAVG)

Uit artikel 9, tweede lid, aanhef en onder g, AVG volgt dat het verbod om bijzondere persoonsgegevens te verwerken, waaronder biometrische, niet van toepassing is indien "de verwerking noodzakelijk [is] om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene".

Artikel 29 UAVG betreft een nationaalrechtelijke uitzonderingsgrond, zoals bedoeld in artikel 9, tweede lid, aanhef onder g, AVG. Deze bepaling bevat een uitzondering voor de verwerking van biometrische gegevens als dat noodzakelijk is voor authenticatie of beveiligingsdoeleinden.

> Zie artikel 29 UAVG:
>
> "Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden."
>
> Zie daarover ook de toelichting op de UAVG; *Kamerstukken II* 2017/18, 34 851, 3, p. 109:
>
> "In de publieke en private sector zijn biometrische systemen sterk in opkomst voor bijvoorbeeld het reguleren van de toegang tot bepaalde plaatsen en gebouwen, maar ook toegang tot informatiesystemen. (…) Het afzien van een nationale uitzondering voor biometrische gegevens zou, gelet op het voorgaande, betekenen dat de bestaande ontwikkelingen in het gebruik van biometrie als identificatiemiddel sterk gehinderd zouden worden. Bestaande verwerkingen van biometrische gegevens, zoals bijvoorbeeld die

> in de relatie tussen werkgever en werknemer zouden hun rechtsgrondslag verliezen. Dit is niet wenselijk."

Dat de verwerking van biometrische gegevens *noodzakelijk* moet zijn voor authenticatie of beveiligingsdoeleinden, houdt in dat de verwerking moet voldoen aan de vereisten van proportionaliteit en subsidiariteit. Voor de proportionaliteitstoets gaat het erom dat er een redelijke en evenwichtige verhouding moet zijn tussen enerzijds het belang bij een goede authenticatie of beveiliging en anderzijds de privacybelangen van de betrokkenen. Voor de subsidiariteitstoets gaat het erom of er geen gebruik kan worden gemaakt van andere, minder ingrijpende methoden voor de authenticatie of beveiliging. Duidelijk is daarbij dat de wetgever de werking van de uitzondering van artikel 29 UAVG heeft willen beperken tot uitzonderlijke situaties waarin de inzet van biometrie wordt gerechtvaardigd door de aanwezigheid van concrete en zwaarwegende veiligheidsrisico's. Zo kan dat wel voor de toegangsverlening aan daartoe bevoegde personen tot een kerncentrale, maar niet voor de toegang van werknemers tot een garagebedrijf.

> Zie de toelichting op de UAVG; *Kamerstukken II* 2017/18, 34 851, 3, p. 109:
>
> "Er dient (…) een afweging te worden gemaakt of identificatie met biometrische gegevens noodzakelijk is voor authenticatie of beveiligingsdoeleinden. De werkgever zal dan moeten afwegen of de gebouwen en informatiesystemen zodanig beveiligd moeten zijn dat dit met biometrie dient plaats te vinden. Dit zal het geval zijn als de toegang beperkt dient te zijn tot bepaalde personen die daartoe geautoriseerd zijn, zoals bij een kerncentrale. Het verwerken van biometrische gegevens dient ook proportioneel te zijn. Als het om de toegang tot een garage van een reparatiebedrijf gaat, zal de noodzaak van de beveiliging niet zodanig zijn dat werknemers alleen met biometrie toegang kunnen krijgen en daartoe deze gegevens worden vastgelegd om de toegangscontrole uit te oefenen. Aan de andere kant kan biometrie soms juist een belangrijke vorm van beveiliging zijn voor bijvoorbeeld informatiesystemen, die zelf veel persoonsgegevens bevatten, waarbij onrechtmatige toegang, ook van werknemers, moet worden voorkomen.
>
> Om deze afweging mogelijk te maken in omstandigheden waarin toestemming niet in vrijheid kan worden gegeven, is in het wetsvoorstel een bepaling opgenomen die een uitzondering op het verbod voor verwerking van biometrische gegevens mogelijk maakt met het oog op de identificatie van de betrokkene, indien dit noodzakelijk is voor authenticatie of beveiligingsdoeleinden."

Artikel 29 UAVG zou op grond van een conceptvoorstel als volgt worden verduidelijkt:[78]

> "Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking

[78] https://www.internetconsultatie.nl/verzamelwetgegevensbescherming.

> noodzakelijk is voor authenticatie of omwille van beveiligingsdoeleinden en slechts voor zover dit noodzakelijk is vanwege een algemeen zwaarwegend belang van rechtmatige toegang tot bepaalde plaatsen, gebouwen, diensten, producten, informatiesystemen of werkprocessystemen."

In de ontwerptoelichting op deze bepaling worden meer voorbeelden gegeven van gevallen waarin de inzet van biometrie voor authenticatie of beveiligingsdoeleinden noodzakelijk is.

> Zie de ontwerptoelichting, p. 15:
>
> "In de toelichting bij dit artikel bij de invoering van de UAVG, werd reeds als voorbeeld van een zwaarwegend algemeen belang de toegang tot een kerncentrale gegeven in tegenstelling tot de toegang van een garage van een reparatiebedrijf. De beveiliging van een kerncentrale is natuurlijk een aansprekend voorbeeld van een zwaarwegend algemeen belang. Maar ook het beschermen van de volksgezondheid, het voorkomen van milieuschade of het beveiligen van vitale processen kunnen redenen zijn waarmee aan de eis van zwaarwegend algemeen belang wordt voldaan. Er zal in ieder geval een belang gediend moeten worden dat uitstijgt boven louter reguliere bedrijfs- of organisatiebelangen (als efficiëntie of kostenbesparing), wil een verwerkingsverantwoordelijke een beroep op deze uitzondering kunnen doen." [onderstreping toegevoegd]

Volledigheidshalve merken wij daarbij op dat met het conceptvoorstel voor de Verzamelwet gegevensbescherming ook een aanscherping van artikel 29 UAVG is beoogd, in de vorm van een dubbele noodzakelijkheidstoets. Bij inwerkingtreding van het nieuwe artikel 29 AVG zou van geval tot geval moeten worden getoetst of de beoogde verwerking van biometrische gegevens noodzakelijk is voor een zwaarwegend algemeen belang.[79]

Een zwaarwegend algemeen belang en rasgegevens (artikel 9, tweede lid, aanhef en onder g, AVG jo. artikel 25, aanhef en onder a, UAVG)

De verwerking van beelden waaruit (indirect) informatie is af te leiden over iemands ras of etniciteit, is op grond van artikel 9, tweede lid, aanhef en onder g, AVG jo. artikel 25, aanhef en onder a, UAVG toegestaan indien de verwerking is gericht op de identificatie van de persoon en deze verwerking voor dat doel onvermijdelijk is. Daarvan is volgens ons bij het aflezen van beelden sprake.

[79] Zie de ontwerptoelichting, p. 15: "Met het in de wettekst opnemen van de eis dat bij het gebruik maken van deze wettelijke uitzondering, het noodzakelijk is ook nog in het concrete geval te toetsen aan het bedoelde zwaarwegend algemeen belang, wordt in een extra waarborg voorzien. In de rechtspraktijk zal een verwerkingsverantwoordelijke nu telkens zelf actief moeten toetsen of ook in het specifieke geval wel aan het vereiste "noodzakelijk voor een zwaarwegend algemeen belang" is voldaan, voordat een beroep op de uitzondering kan worden gedaan. Deze afweging zal vervolgens door de AP en uiteindelijk ook door de rechter worden beoordeeld." [onderstreping toegevoegd]

6.1.5 Uitzonderingsgronden voor strafrechtelijke persoonsgegevens

Voor strafrechtelijke persoonsgegevens geldt dat deze alleen mogen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan op grond van het Unierecht of nationaal recht, en passende waarborgen worden geboden voor de rechten en vrijheden van de betrokkenen. De algemene uitzonderingsgronden zijn in het nationale recht in artikel 32 en 33 AVG neergelegd. Daarnaast kan sectorspecifieke wetgeving uitzonderingen bevatten.

6.2 Grondslagen voor de onderhavige verwerkingen?

6.2.1 Fase 1 − Signaleren van discriminatie en racisme

Wettelijke grondslag

Wij achten het in algemene zin goed verdedigbaar dat de met de inzet van slimme technologieën gepaarde gegevensverwerking kan worden gebaseerd op het gerechtvaardigde belang van de BVO om onrechtmatig gedrag − waaronder discriminatie en racisme − tegen te gaan. Daarbij stellen wij voorop dat de AP in haar normuitleg heeft onderkend dat vergelijkbare belangen − het borgen van een veilig leven in een dreigende situatie, het tegengaan van inbreuken op persoonlijkheidsrechten, het tegengaan van onrechtmatig gedrag en het nakomen van zorgplichten − als gerechtvaardigde belangen als bedoeld in artikel 6, eerste lid, aanhef en onder f, AVG kunnen kwalificeren.

Ook valt volgens ons te onderbouwen dat de belangen van de BVO, van de KNVB en van de voetbalspelers of supporters die het mikpunt zijn van racisme of discriminatie zwaarder wegen dan het privacybelang van de betrokken supporters. Aandachtspunt is daarbij wel dat de gevolgen van de inzet van de slimme technologie − uiteraard afhankelijk van het ontwerp en de aard van de technologie − vergaand kunnen zijn. Het is tegen deze achtergrond van belang dat de BVO aanvullende waarborgen per technologie treft om onevenredige gevolgen voor de betrokkenen te voorkomen. Wij zullen een en ander nader toelichten onder het hiernavolgende kopje ‘Noodzakelijkheid’.

Daarnaast zal de BVO zorgvuldig en gedegen de noodzaak van de inzet van (een combinatie van) slimme technologie (in aanvulling op reeds bestaande middelen) moeten onderbouwen. Ook daarbij staan wij hierna uitgebreider stil onder het kopje ‘Noodzakelijkheid’.

Doorbrekingsgrond voor verwerking bijzondere persoonsgegevens

Op voorhand lijken er met de inzet van slimme camera’s en microfoons geen bijzondere persoonsgegevens te worden verwerkt, omdat dat in deze fase niet is gericht op identificatie van betrokkenen dan wel anderszins gericht op (het maken van

onderscheid op grond van) bijzondere persoonsgegevens. Voor zover er (toch) bijzondere persoonsgegevens worden verwerkt met de slimme camera's en microfoons in deze fase en dat geschiedt met oog op de identificatie van betrokkenen (zie fase 2), menen wij dat een grondslag bestaat in artikel 25, aanhef en onder a, UAVG.

Daarbij zij benadrukt dat emotieherkenning géén biometrisch gegeven betreft, aangezien emotieherkenning (ook) niet is gericht op de identificatie van een persoon dan wel anderszins op bijzondere persoonsgegevens, maar op het herkennen en signaleren van discriminerende en racistische uitlatingen.

Wettelijke grondslag voor de verwerking van strafrechtelijke persoonsgegevens

Aangezien de inzet van slimme technologie specifiek tot doel heeft om dergelijk gedrag te signaleren en identificeren, zullen voetbalclubs niet kunnen uitsluiten dat bij de inzet van slimme technologie beelden worden vastgelegd die een dergelijke (strafrechtelijke) verdenking kunnen dragen. Dit maakt dat de voetbalclub dient te beschikken over een expliciete grondslag als bedoeld in artikel 10 AVG, respectievelijk de artikelen 31 − 33 UAVG. De meest realistische grondslag voor de verwerking van strafrechtelijke persoonsgegevens betreft artikel 33, vierde lid, aanhef en onder c, AVG dat bepaalt dat een dergelijke verwerking is toegestaan indien de AP daarvoor een vergunning heeft verleend. Een dergelijke vergunning wordt verleend indien de verwerking noodzakelijk is met het oog op een zwaarwegend algemeen belang van derden en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. De AP kan aan de vergunning voorschriften verbinden. Gezien het met de inzet van de slimme technologie nagestreefde doel (bestrijden van racistisch en discriminerend gedrag) is onze inschatting dat het zwaarwegend algemeen belang in voldoende mate door de voetbalclub zal kunnen worden onderbouwd. Ook de noodzaak voor de inzet van slimme technologie achten wij aanwezig (zie keuzeladder hierna). Wij raden voetbalclubs aldus aan om eerst met de AP in gesprek te gaan over het verkrijgen van een vergunning voor het verwerken van strafrechtelijke persoonsgegevens, voordat de slimme technologie wordt ingezet. Voor specifieke situaties zou ook artikel 33, tweede lid, aanhef en onder b, UAVG uitkomst kunnen bieden. Aangezien het hier gaat om een gelijkluidende vergunning zouden de BVO ervoor kunnen kiezen om (vanuit praktische redenen) een gezamenlijke vergunningsaanvraag te starten. Daarvoor is overigens wel vereist dat de BVO's de vertegenwoordiger daartoe volmachten.

Artikel 33, tweede lid, aanhef en onder b, UAVG bepaalt dat een verwerkingsverantwoordelijke strafrechtelijke persoonsgegevens mag verwerken ter bescherming van zichzelf met betrekking tot (gepleegde of te plegen) strafbare feiten jegens hem of zijn werknemers. De verwerking van beelden van racistische of discriminerende uitingen die zijn gericht tegen de eigen werknemers van de voetbalclub zou op deze grondslag kunnen worden gebaseerd.

Wij achten deze grondslag echter minder goed bruikbaar dan het aanvragen van een vergunning bij de AP, aangezien deze bepaling slechts de verwerking ten eigen behoeve van de voetbalclub rechtvaardigt. De verstrekking van beelden (die gezien de aard van de beelden kwalificeren als strafrechtelijke persoonsgegevens) aan anderen (waaronder de KNVB of de politie) kan niet op deze grondslagen worden gebaseerd. Daarbij geldt bovendien dat de BVO deze grondslag enkel kan inroepen ter bescherming van zichzelf of zijn eigen werknemers. Ook in zoverre is de bruikbaarheid van deze doorbrekingsgrondslag beperkt.

Noodzakelijkheid

Wij zien in algemene zin voldoende argumenten voor de inzet van slimme technologieën, mits BVO's de noodzaak daarvan met voldoende feiten kunnen onderbouwen (en dat vervolgens ook zorgvuldig motiveren) en voldoende maatregelen treffen om de omvang en aard van de verwerking te beperken tot het strikt noodzakelijke. Uitgaande van de beperkingen waar de voetbalclubs bij het gebruik van bestaande middelen tegenaan lopen bij de signalering van racisme en discriminatie (met name gezien de technische beperkingen die samenhangen met vaak verouderede camera's), zou betoogd kunnen worden dat (een combinatie van) slimme technologie effectiever zal zijn in het signaleren van discriminatie en racisme. Om de proportionaliteit van de keuze voor slimme technologie te kunnen rechtvaardigden, dient de voetbalclub evenwel steeds zorgvuldig de strikte noodzaak te onderbouwen. Ook dient de voetbalclub waar nodig de slimme technologieën zo in te stellen dat de privacyinbreuk voor betrokkenen zo veel mogelijk wordt beperkt tot het strikt noodzakelijke (privacy by design & default). Pas als voetbalclubs in deze onderbouwing slagen, achten wij een keuze voor een slimme technologie gerechtvaardigd. Wij lichten dit nader toe.

Wij stellen voorop dat de door ons geïnterviewde voetbalclubs weliswaar vergelijkbare procedures kennen, maar de (door de KNVB voorgeschreven) video-installaties die worden ingezet van wisselende kwaliteit zijn. Uitgangspunt is daarom dat iedere BVO eerst zal moeten motiveren waarom de huidige technieken op dit moment onvoldoende zijn in de signalering van discriminatie en racisme. Onderdeel van deze analyse zou ook een beschrijving moeten zijn van eerdere incidenten die betrekking hadden op racisme en discriminatie, evenals een inschatting of de keuze voor de slimme technologie naar verwachting zal leiden tot een verbetering van de signalering van discriminatie en racisme. Waar mogelijk verdient het aanbeveling om met wetenschappelijke onderzoeken te motiveren dat de inzet van de slimme technologieën een positief effect zal hebben op deze signalering. Mocht dergelijk wetenschappelijk onderzoek ontbreken, zouden de voetbalclubs de keuze voor een slimme technologie kunnen onderbouwen met ervaringsregels, bijvoorbeeld door te verwijzing naar ervaringen bij clubs die reeds verder zijn in de ontwikkeling van hun videosysteem of reeds werken met slimme technologieën.

Wij wijzen erop dat vanuit het beginsel van subsidiariteit in beginsel eerst moet worden volstaan met maatregelen die een beperkte inbreuk maken op de privacy van betrokkenen en pas wordt gekozen voor zwaardere middelen (waaronder slimme technologieën) indien kan worden aangetoond dat de lichte middelen onvoldoende zijn om racisme en discriminatie aan te pakken. Om voetbalclubs te helpen bij hun keuze lichten wij in de hierna volgende 'keuzeladder' toe welke aspecten voetbalclubs en de KNVB in hun afwegingen zouden moeten meenemen. Ook zullen wij per technologie aanbeveling doen voor de technische maatregelen die getroffen kunnen worden ter waarborg van de beginselen van privacy by design & default.

Keuzeladder

Relatief lage privacyinbreuk Relatief hoge privacyinbreuk

(a) Signalering door scheidsrechters, grensrechters, officials en stewards

De minst inbreuk makende maatregel is het door de scheidsrechter, grensrechter, officials of stewards real-time constateren van racistische en discriminerende uitingen. De indruk bestaat dat deze vorm van (louter) menselijke signalering onvoldoende is om discriminatie en racisme in voetbalstadions daadwerkelijk goed te kunnen signaleren.

(b) Gebruik en verbetering van reeds bestaande videosystemen (zonder slimme technologie)

Op dit moment zetten BVO's reeds video-installaties in voor het vaststellen van ongeregeldheden binnen de supportersvakken. Zoals toegelicht in paragraaf 3.1.1. van dit rapport, heeft de KNVB de inzet van deze video-installaties voorgeschreven middels licentie-eisen. In de praktijk gaat het vaak om beveiligingscamera's van wisselende kwaliteit. Voordat wordt overgegaan tot de inzet van slimme(re) camera's en microfoons is van belang dat BVO's nagaan of verbetering van de kwaliteit van deze video-installaties al tot de gewenste verbetering van signaleringsmogelijkheden kan leiden. De voetbalclub zou pas moeten overgegaan tot zwaardere middelen, voor zover kan worden aangetoond dat de opnames met de video-installaties onvoldoende zijn om discriminatie en racisme te signaleren. Wij zien daar op dit moment goede argumenten voor. Een belangrijk aandachtspunt is bijvoorbeeld het beter synchroniseren van beeld en geluid, zodat kan worden vastgesteld wie de uitlatingen heeft gedaan.

Technische en organisatorische waarborgen en suggesties privacy by design & default

Voor zover wordt volstaan met het gebruik van de (eventueel verbeterde) reeds bestaande videosystemen (zonder slimme technologie) geldt ook hier dat de nodige maatregelen kunnen worden getroffen om de strikte noodzaak van de verwerking en de beginselen van privacy by design & default te borgen. Daarbij kan gedacht worden aan de volgende maatregelen:

- Stel de camera's zo in dat in beginsel ieder vak wordt gefilmd, maar borg dat enkel de relevante beelden worden geselecteerd voor nader onderzoek.
- Bewaar de verkregen beelden en de persoonsgegevens voor een beperkte, strikt noodzakelijke termijn.
- Beperk de omvang van de personen die toegang hebben tot beelden tot het strikt noodzakelijke. Een en ander dient te worden uitgewerkt in een concreet autorisatiebeleid. Werk in dit beleid waar mogelijk uit wanneer nader onderzoek ten behoeve van de signalering van discriminatie of racisme mag worden overgegaan.
- Overweeg een evaluatieprotocol op te stellen, waarmee de BVO doorlopend kan bezien of het gebruik van de bestaande videosystemen voldoende effectief zijn. Voor zover zich signalen voordoen dat de effectiviteit of de bewijswaarde van de bestaande videosystemen te wensen overlaat, kunnen deze evaluaties als grondslag dienen voor de keuze van meer ingrijpende slimme technologieën.

(c) Slimme camera's en microfoons

Pas op het moment dat (de combinaties van) de achter (a) en (b) genoemde maatregelen (aantoonbaar) onvoldoende zijn om racisme en discriminatie bij voetbalwedstrijden aan te pakken, zou de voetbalclub in overweging kunnen nemen om te kiezen voor slimme camera's en microfoons (inclusief spraakherkenning). Daarbij dient te worden bedacht dat de soort slimme camera en de gekozen instellingen van invloed zullen zijn op de inbreuk op de privacy van betrokkenen.

Onze inschatting is dat de inzet van slimme camera's en microfoons een noodzakelijke en proportionele maatregel zou kunnen vormen voor het bestrijden van discriminatie en racisme. Van belang daarbij is dat de slimme camera's en de slimme geluidsdetectie zo wordt ingesteld en getraind dat deze zoveel mogelijk alleen relevante beelden en geluiden registeren. Dit houdt onder meer in dat beelden en geluiden die niet relevant zijn niet worden opgenomen, dan wel gepseudonimiseerd worden bewaard en zo snel mogelijk worden verwijderd. Het zijn specifiek dergelijke instellingen die in het concrete geval zullen bepalen of de gekozen slimme technologie daadwerkelijk proportioneel kan worden geacht. De AP overweegt daarover in zijn beleidsregels cameratoezicht het volgende:

> "Cameratoezicht door middel van slimme camera's kan tot gevolg hebben dat er een minder vergaande inbreuk op de persoonlijke levenssfeer wordt gemaakt dan door middel van 'reguliere' camera's.125 Zo zullen de camerabeelden vaak pas worden bekeken wanneer de slimme camera's iets detecteren. De inbreuk op de persoonlijke levenssfeer wordt nog kleiner wanneer de slimme camera's pas beelden gaan *opnemen* zodra ze iets detecteren (dataminimalisatie).
>
> Aan de andere kant kan de inzet van slimme camera's juist ook tot gevolg hebben dat er sprake is van een grotere inbreuk op de persoonlijke levenssfeer. Camera's met gezichtsherkenning kunnen bijvoorbeeld personen op geautomatiseerde wijze traceren, volgen en profileren, hetgeen met reguliere camera's niet mogelijk is. Camera's die zijn uitgerust met een techniek voor gedragsanalyse, analyseren voorts de gedragingen van een ieder die in beeld komt. De gedragingen van die personen worden dus geanalyseerd zonder dat zij iets 'fout' hoeven te hebben gedaan. Bovendien hebben de camera's geen verstand en intuïtie, zodat gedragingen gemakkelijk verkeerd kunnen worden geïnterpreteerd."

Wij wijzen erop dat de slimme camera's en microfoons niet slechts privacygevoelig zijn in de toepassing, maar ook in de ontwikkeling en training van de beelden. Voor de ontwikkeling en training van slimme camera's en microfoons zal naar verwachting statistisch onderzoek noodzakelijk zijn. Een dergelijk statistisch onderzoek dient te voldoen aan zeer strikte vereisten. Wij wijzen daarbij op paragraaf 6.1.4 van dit rapport en bijlage 1 van dit rapport. Er zal een grote hoeveelheid (persoons)gegevens nodig zijn om de slimme technologieën discriminatie en racisme te laten herkennen. Dit vormt een relevant aspect bij de keuze voor een dergelijke technologie. Indien er in het kader van het trainen of ontwikkelen van het algoritme bijzondere persoonsgegevens moeten worden verwerkt, zodat bijv. racistische handelingen effectiever herkend worden, dan moet worden voldaan aan randvoorwaarden van artikel 24 UAVG.

Technische en organisatorische waarborgen en suggesties privacy by design & default

Voor zover wordt gekozen voor deze vormen van slimme technologie dienen verdergaande maatregelen te worden getroffen om de strikte noodzaak van de verwerking en de beginselen van privacy by design & default te borgen. Daarbij kan gedacht worden aan de volgende maatregelen en waarborgen:

- Stel waar mogelijk de slimme camera's en microfoons zo in dat minder opnames worden gemaakt in vergelijking tot de achter (b) genoemde camerabeelden, bijvoorbeeld door de apparatuur zo in te stellen dat zij pas gaat opnemen en opslaan zodra racisme en discriminatie wordt gedetecteerd. Voor zover het niet mogelijk of wenselijk is dat de camera's pas bij een specifiek incident van start gaan met het daadwerkelijk registreren van de beelden of het geluid, zou de BVO het vaste beleid moeten hanteren dat de beelden versleuteld worden opgeslagen en slechts de door de slimme

technologie geselecteerde beelden van onregelmatigheden worden getoond aan de desbetreffende medewerker. Dit in verband met het dataminimalisatiebeginsel.

- Gebruik slechts slimme technologieën waarvoor in voldoende mate wetenschappelijk onderzoek bestaat over de effectiviteit van de technologie, evenals informatie over de validatie van het achterliggende algoritme en verificatie van de aan het algoritme ten grondslag liggende factoren. Uit deze informatie moet in ieder geval blijken welke stappen genomen zijn in de ontwikkeling en validatie van de indicatoren van de technologieën (en of en door wie deze zijn ge-peerreviewed), alsook welke statistische trainingsmodellen gebruikt zijn.

- Licht in een verantwoordingsdocument (waar mogelijk) toe hoe de selectie van de beelden het geluid plaatsvindt en motiveer daarbij standaard wat de daarvan de onderliggende variabelen zijn.

- Overweeg ook hier een evaluatieprotocol op te stellen, waarmee de BVO doorlopend kan bezien of het gebruik van de slimme technologie voldoende effectief is. Voor zover zich signalen voordoen dat de effectiviteit of de bewijswaarde van de bestaande videosystemen te wensen overlaat, kunnen deze evaluaties als grondslag dienen voor de keuze van meer ingrijpende slimme technologieën.

- Zorg ervoor dat − naast het enkele gebruik van de slimme technologieën − periodiek handmatig gedurende een wedstrijd discriminerende of racistische uitlatingen worden geselecteerd. Op deze manier kan worden gecontroleerd of de slimme technologieën juist staan afgesteld. Eventuele discrepanties zouden aanleiding kunnen vormen onderzoek te doen naar of de slimme technologie niet naar behoren functioneert of niet juist is afgesteld.

(d) Slimme camera’s met emotieherkenning

De in onze optiek meest privacygevoelige soort slimme camera’s betreft camera’s met emotieherkenning. Wij betwijfelen de noodzaak van de inzet van emotieherkenning. Eerst zou moeten worden aangetoond dat controle van de (door slimme technologie geselecteerde) beelden en geluid niet handmatig of door middel van de achter (c) genoemde middelen kunnen worden geanalyseerd. Onze twijfel aan de noodzaak is mede ingegeven door de omstandigheid dat emotieherkenning − gezien de huidige stand van de techniek en gezien de vaststelling dat discriminatie niet altijd gekoppeld is aan een specifieke emotie − slechts een beperkte aanvullende meerwaarde zal hebben ten opzichte van de achter (c) genoemde slimme technieken. Dat is ook in de marktverkenning onderkend.

Verdere verwerking / doelbinding

In de BVO's gehanteerde (en door de KNVB voorgeschreven) algemene voorwaarden wordt in artikel 9.2 beschreven dat camerabeelden worden gemaakt van de supporters die tijdens een wedstrijd aanwezig zijn. Uit de algemene voorwaarden maken wij op dat de verwerking van de camerabeelden verschillende doeleinden hebben, waaronder (i) commerciële doeleinden (de uitzending van de wedstrijd) en (ii) het controleren van deze beelden ten behoeve van het vaststellen van onrechtmatig gedrag als beschreven in artikel 8 van de algemene voorwaarden, en de sanctieoplegging van overtreders als bedoeld in artikel 10 van de algemene voorwaarden. Gelet daarop gaan wij ervan uit dat de verwerking van opnames ten behoeve van het signaleren van discriminatie en racisme een primaire verwerking betreft voor zover de beelden worden verwerkt voor eigen gebruik van de BVO. In zoverre is van een 'verdere verwerking' geen sprake en hoeft niet te worden voldaan aan de eisen van artikel 6, vierde lid, AVG.

Het verstrekken van verkregen beelden aan derden (ten behoeve van het opleggen van een sanctie), waaronder bijvoorbeeld aan de KNVB of de politie, betreft wel een verdere verwerking. In paragraaf 6.2.3 gaan wij in op de rechtmatigheid daarvan.

Casus inzet slimme technologie – Signaleringsfase

De BVO heeft ervoor gekozen om ter bestrijding van discriminatie en racisme binnen het voetbalstadion slimme camera's te plaatsen die op een geautomatiseerde wijze (potentiële) discriminerende of racistische gedragingen door toeschouwers herkent en registreert. De inzet van deze slimme technologie is gerechtvaardigd, omdat de voetbalclub – mede overeenkomstig de in dit rapport opgenomen keuzeladder – heeft gemotiveerd dat minder ingrijpende maatregelen geen uitkomst bieden (zie optie c van de keuzeladder signaleringsfase). De BVO heeft in overleg met de AP een vergunning aangevraagd voor het verwerken van eventuele strafrechtelijke persoonsgegevens die met de slimme technologie worden verwerkt.

De veiligheidscoördinator stelt na afloop van de wedestrijd vast dat vijf personen op de tribune een racistisch spreekkoor inzetten. De veiligheidscoördinator stelt vast dat uit de geluidsfragmenten twee uitingen zijn af te leiden. Door inzet van slimme geluidsanalyse (in combinatie met technologie waarmee kan worden vastgesteld wie op dat moment de desbetreffende leus uitsprak) kan met voldoende zekerheid worden vastgesteld dat twee mannen de desbetreffende leuzen hebben geroepen. Zij maken zich schuldig aan twee vormen van racistisch gedrag:

- Ten eerste worden er uitingen gedaan over de huidskleur van een speler van de tegenpartij. Dit betreft racistisch gedrag gericht tot één specifiek persoon. De inschatting van de veiligheidscoördinator is dat deze uitingen vallen aan te merken als (individuele) belediging van de desbetreffende speler.
- Ten tweede stelt de veiligheidscoördinator vast dat de mannen racistische leuzen schreeuwen over een religieuze bevolkingsgroep. De veiligheidscoördinator vermoedt dat deze uitingen zijn aan te merken als groepsbelediging.

Aangezien de beelden aanleiding vormen voor nader onderzoek, slaat de veiligheidscoördinator de beelden en geluidsfragmenten (evenals het dossier met daarin de voorlopige bevindingen) op in de KVV. Daarmee komt de signaleringsfase ten einde.

(zie bijlage 3 voor de volledige casus (signalering – identificatie – sanctie))

6.2.2 Fase 2 − Identificeren van de betrokkene

Wettelijke grondslag

Ook voor de inzet van slimme technologieën ten behoeve van de identificatie van de betrokkene, menen wij dat het gerechtvaardigde belang van de voetbalclub, KNVB en/of de supporters of spelers die het mikpunt zijn van de uitlatingen, een grondslag kunnen vormen voor de verwerking van persoonsgegevens (artikel 6, eerste lid, aanhef en onder f, AVG). Wij verwijzen hier naar paragraaf 6.1.1 van dit hoofdstuk.

Doorbrekingsgronden voor de verwerking van bijzondere persoonsgegevens

Hoewel in de identificatiefase de inzet van gezichtsherkenningstechnologie zou kunnen bijdragen aan de vaststelling van de identiteit van de potentiële dader (en daarmee aan de bewijsvoering in de sanctiefase), lijkt een toereikende doorbrekingsgrond daarvoor te ontbreken. Zoals toegelicht in paragraaf 6.1.4, kunnen op grond van artikel 29 UAVG biometrische gegevens worden verwerkt als dat noodzakelijk is voor authenticatie en beveiligingsdoeleinden, en ligt de noodzakelijkheidslat daarbij hoog. De uitzonderingsgrond lijkt vooral te zijn bedoeld voor de authenticatie en beveiliging van plaatsen met een hoog risico op veiligheidsincidenten. Wij hebben sterke twijfel − mede gelet op de voorgenomen verduidelijking van het artikel in het conceptwetsvoorstel − of de bepaling ook bedoeld is voor het voorkomen van discriminatie en racisme in een voetbalstadion.

Gezien de huidige kwaliteit van, naar wij begrijpen, een relevant deel van de camera's van BVO's zijn wij er (vooralsnog) ook niet van overtuigd dat er een strikte noodzaak zou bestaan om gezichtsherkenningstechnologie in te zetten ten behoeve van de identificatie van personen. Uit de interviews maken wij op dat − naar verwachting − een verbetering van de camera's (en de koppeling van beelden met geluid) de signaleringsmogelijkheden van racisme en discriminatie zal vergroten.

Daar komt bij dat vooralsnog niet is aangetoond dat andere, minder ingrijpende middelen niet toereikend zouden zijn. Gedacht kan bijvoorbeeld worden aan handmatige identificatie in combinatie met stoelnummerregistratie en/of registratie met een foto vooraf. Zolang niet kan worden aangetoond dat dergelijke minder ingrijpend middelen niet toereikend zijn voor de effectieve bestrijding van discriminatie en racisme, kan geen beroep worden gedaan op artikel 29 UAVG. Wij menen dan ook dat vooralsnog niet gekozen kan worden voor de inzet van gezichtsherkenningstechnologie op grond van artikel 29 UAVG. Datzelfde geldt onzes inziens voor de inzet van stemherkenningstechnologie.

Wij vinden steun voor deze conclusie in een recente uitspraak van de Rechtbank Amsterdam over de vraag of een schoenenwinkel bevoegd is om werknemers te verplichten tot het gebruik van een vingerscan voor het kassasysteem.[80] De

[80] Rb. Amsterdam 12 augustus 2019, ECLI:NL:RBAMS:2019:6005.

kantonrechter oordeelde dat het door de schoenenwinkel gestelde bedrijfsbelang (het bestrijden van fraude door het eigen personeel en de daarmee gepaarde omzetderving) géén type bedrijfsbelang is dat is aan te merken als noodzakelijk voor authenticatie of beveiligingsdoeleinden. Het door de schoenenwinkel gestelde belang om gevoelige informatie die via het kassasysteem toegankelijk is te beschermen, acht de kantonrechter wél een belang dat door artikel 29 UAVG wordt beschermd.[81] In het concrete geval van Manfield acht de kantonrechter het invoeren van de vingerscan echter in strijd met het noodzakelijkheidsbeginsel. Manfield heeft onvoldoende (door middel van documenten) aangetoond dat andere minder ingrijpende alternatieven voorhanden zijn om de persoonsgegevens in het kassasysteem te beschermen.

Daarnaast heeft de Franse privacytoezichthouder Commission nationale de l'informatique et des libertés ('CNIL') recent een sportclub gewaarschuwd over het gebruik van gezichtsherkenningstechnologie in een stadion.[82] Die technologie zou worden ingezet ten behoeve van de handhaving van stadionverboden, onderzoek naar voorwerpen en de strijd tegen terrorisme. Volgens de CNIL is de inzet van gezichtsherkenningstechnologie in beginsel verboden en zijn in het betreffende geval andere middelen voorhanden om genoemde doelen te bereiken.

De uitdrukkelijke toestemming van toeschouwers (artikel 9, tweede lid, aanhef en onder a, AVG) kan naar verwachting de doorbreking van het verbod op de verwerking van bijzondere persoonsgegevens niet rechtvaardigen. Onzeker is of er in deze situatie kan worden gesproken van vrije toestemming van de toeschouwers. Om tot het stadion toegang te krijgen is toestemming vereist. Er kan derhalve worden gezegd dat het weigeren van de toestemming een nadelig gevolg heeft voor de toeschouwer – hij komt het stadion niet in. En dat brengt met zich mee dat gezegd kan worden dat het onzeker is of deze toestemming in vrijheid is gegeven. Dit sluit aan bij de opvatting van de AP. Van de daartoe vereiste vrijelijke toestemming is volgens de opvatting van de AP geen sprake, aangezien de toestemming afhankelijk wordt gemaakt van de toegang tot het voetbalstadion en het accepteren van de algemene voorwaarden van de door de KNVB en de voetbalclub gestelde eisen.[83]

Hoewel wij dus niet zonder meer een grondslag zien voor het doorbreken van het verbod op de verwerking van bijzondere persoonsgegevens (waaronder biometrische gegevens), bestaan er wel steeds meer speciale technieken die kunnen worden ingezet om de privacy van betrokkenen bij de inzet van gezichtsherkenning te waarborgen. Wij verwijzen in dit verband naar het TNO-rapport "Privacy bescherming bij niet-coöperatieve gezichtsherkenning', waarin wordt toegelicht dat met 'multi-party

---

81 Het gaat daarbij om gegevens die betrekking hebben op financiën, persoonsgegevens van klanten en persoonsgegevens van werknemers. Uit de uitspraak volgt niet dat in het kassasysteem bijzondere persoonsgegevens worden verwerkt die door de inzet van biometrie worden beschermd.

82 Zie https://www.cnil.fr/fr/reconnaissance-faciale-et-interdiction-commerciale-de-stade-la-cnil-adresse-un-avertissement-un-club.

83 Zie ook de formele waarschuwing van de AP aan een supermarkt, waarin wordt gesteld dat het ten behoeve van een commerciële dienst binnenstappen van een supermarkt niet geldt als uitdrukkelijke toestemming. https://autoriteitpersoonsgegevens.nl/nl/nieuws/formele-waarschuwing-ap-aan-supermarkt-om-gezichtsherkenning

computation' biometrische gezichtstemplates op een veiligere manier kunnen worden vergeleken zodat de privacy van betrokkenen zoveel mogelijk wordt geborgd. Hoewel wij ons kunnen vinden in de conclusie dat daarmee het beginsel van dataminimalisatie wordt geborgd, maken dergelijke (privacy waarborgende) technieken niet dat een beroep kan worden gedaan op de doorbrekingsgrond van artikel 29 UAVG. Deze uitzondering strekt immers tot de authenticatie van personen ten behoeve van de beveiliging van plaatsen met een hoog risico op veiligheidsincidenten.

Ten aanzien van identificatie middels stoelnummerregistratie in combinatie met de in fase 1 verkregen beelden, merkten wij in paragraaf 4.2.2 op dat dat geen verwerking van bijzondere persoonsgegevens hoeft te betreffen. Voor zover daarover discussie zou ontstaan, is er een doorbrekingsgrond aanwezig voor de onvermijdelijke verwerking van eventuele (indirecte) ras of etniciteitsbeelden die zichtbaar zijn op de beelden of uit geluidsfragmenten blijken. De verwerking van dergelijke beelden met persoonsgegevens over iemands ras of etniciteit is op grond van de UAVG namelijk toegestaan indien de analyse plaatsvindt met het oog op de identificatie van de desbetreffende persoon, en slechts voor zover de verwerking voor dat doel onvermijdelijk is (artikel 25, aanhef en onder a, UAVG).

Noodzakelijkheidsbeginsel

Ook in de identificatiefase geldt dat voldoende argumenten bestaan voor de inzet van slimme technologieën. BVO's zullen zorgvuldig de inzet van slimme technologieën, daar waar dat juridisch mogelijk is, moeten kunnen onderbouwen en voldoende maatregelen moeten treffen om de omvang en aard van de verwerking te beperken tot het strikt noodzakelijke. Ook in deze fase zal de BVO in een verantwoordingsdocument haar keuze moeten (kunnen) rechtvaardigen. Wij komen tot de volgende keuzeladder.

Wij benadrukken daarbij dat men niet toekomt aan een noodzakelijkheidstoets indien een doorbrekingsgrondslag ontbreekt, zoals vooralsnog het geval lijkt te zijn voor de inzet van gezichtsherkenningstechnologie.

Keuzeladder

Relatief lage privacyinbreuk — Relatief hoge privacyinbreuk

(a) Handmatige (realtime) identificatie van personen

De minst ingrijpende maatregel is de handmatige of realtime analyse van de (eventueel met slimme technologie in fase 1) verkregen beelden en de handmatige identificatie van personen. Wij achten dit middel (relatief) privacyvriendelijk, omdat hiervoor geen pregistratie van (bijvoorbeeld) NAW-gegevens en/of foto's nodig is. Tegelijkertijd is voor de handmatige identificatie in de regel veel mankracht vereist.

Het is bovendien voor de voetbalclubs in veel gevallen moeilijk om personen buiten de vaste supporterskern te kunnen identificeren. Deze vaststelling kan in onze optiek rechtvaardigen dat zwaardere middelen worden ingezet om identificatie van personen mogelijk te maken, bijvoorbeeld door de preregistratie te verbeteren.

Daarbij merken wij op dat voor de hierna beschreven middelen steeds (een vorm van) preregistratie nodig is. Iemand die zich niet wil registreren, kan, als deze preregistratiemiddelen worden ingezet, mogelijk geen toegang meer krijgen tot wedtrijden. Dat heeft implicaties voor de vrije toegang tot betaald voetbalwedstrijden. Dat betreft evenwel een praktisch en/of commercieel aspect, en geen juridisch aspect.[84] De praktische onwenselijkheid van pre-regsitratie laten wij hierom verder buiten beschouwing.

(b) Handmatige identificatie van personen met pre-registratie

Een relatief zwaarder middel zou zijn dat de voetbalclubs ervoor kiezen om de preregistratie te verbeteren, zodat op basis van de beelden van het vastgelegde incident het stoelnummer kan worden gekoppeld aan de persoonsgegevens die vooraf zijn geregistreerd voor die stoelnummers. Bij deze werkwijze moet worden onderkend dat sprake is van een foutmarge, in die zin dat degene die zich met een bepaald stoelnummer heeft geregistreerd van plaats kan zijn gewisseld en/of omdat het mogelijk is om voor meerdere personen kaartjes te kopen voor een vak en onderling is gewisseld. Ook zullen toeschouwers niet altijd op hun plek zitten, maar soms ook staan of rondlopen. Evenwel kan in dat geval via degene die zich heeft geregistreerd op een bepaald stoelnummer wel getracht worden de identiteit van de mogelijke dader van discriminatie of racisme te achterhalen.

(c) Handmatige identificatie van personen met preregistratie inclusief een foto

Indien kan worden onderbouwd dat het gebruik van een foto de effectiviteit en de betrouwbaarheid van de identificatie aanzienlijk vergroot, kan in onze optiek worden gekozen voor het maken van beelden van personen bij de ingang van de voetbalstadions.

Technische en organisatorische waarborgen en suggesties privacy by design & default

Voor zover wordt gekozen voor deze technologie kunnen de volgende maatregelen worden getroffen om de strikte noodzaak van de verwerking en de beginselen van privacy by design & default te borgen.

- Om de inbreuk op de privacy van betrokkenen te beperken tot het strikt noodzakelijke zouden de gegevens die worden verzameld bij de preregistratie

[84] Dat zou anders zijn als de (persoonsgegevens die worden verwerkt bij) preregistratie zou zijn gebaseerd op de toestemming van de toeschouwer als bedoeld in artikel 6, eerste lid, aanhef en onder a, AVG. Dat is niet het geval. Voor de verwerkingen kan, zoals hierboven aangegeven, een grondslag worden gevonden in het gerechtvaardigd belang als bedoeld in artikel 6, eerste lid, aanhef en onder f, AVG.

versleuteld kunnen worden opgeslagen, totdat op basis van de beelden aanleiding bestaat om nader onderzoek te verrichten naar personen op specifieke stoelnummers. De relevante stoelnummers (incl. de foto van de personen die bij de toegangspoort hun kaartjes hebben laten scannen) zouden vervolgens kunnen worden ontsloten ten behoeve van het onderzoek.

- Van belang is tot slot dat de versleutelde dataset (met daarin de bij de toegang gemaakte foto's gekoppeld aan het stoelnummer op het kaartje) geautomatiseerd wordt verwijderd op het moment dat geen nader onderzoek meer noodzakelijk is.

(d) Biometrische identificatie

De meest privacygevoelige keuze zou de inzet van gezichts- en/of stemherkenningstechnologie zijn. In dat geval worden de opgenomen beelden (en eventueel ook geluiden) geautomatiseerd door middel van biometrische toepassingen geanalyseerd en worden betrokkenen op basis van die analyse geïdentificeerd. Op dit moment zien wij daar geen toereikende (doorbrekings)grondslag voor.

Zoals reeds toegelicht bij 'doorbrekingsgrond voor de verwerking van bijzondere persoonsgegevens' van dit hoofdstuk, zien wij (vooralsnog) geen toereikende doorbrekingsgrond of strike noodzaak om biometrische toepassingen in te zetten.

Verdere verwerking / doelbinding

Ook de verwerking van persoonsgegevens met het oog op het identificeren van betrokkenen betreft onzes inziens een primaire verwerking voor zover de BVO dat voor eigen gebruik doet (vergelijk de conclusie onderaan paragraaf 6.2.1 hierboven). In zoverre is van een 'verdere verwerking' geen sprake en hoeft niet te worden voldaan aan de eisen van artikel 6, vierde lid, AVG.

Het verstrekken van verkregen beelden aan derden (ten behoeve van het opleggen van een sanctie), waaronder bijvoorbeeld aan de KNVB of de politie, betreft wel een verdere verwerking. In paragraaf 6.2.3 gaan wij in op de rechtmatigheid daarvan.

Casus inzet slimme technologie – Identificatiefase

Nadat de veiligheidscoördinator de twee vormen van racistisch gedrag (individuele belediging speler en groepsbelediging) heeft gesignaleerd, gaat de veiligheidscoördinator over tot een nadere analyse van de beelden. Het doel daarvan is het identificeren van de twee mannen. Bij veel voetbalclubs zal de identificatie handmatig gaan. De voetbalclub waar de veiligheidscoördinator werkzaam is heeft echter recentelijk – overeenkomstig de keuzeladder voor de identificatiefase – ervoor gekozen om de kaartverkoop te koppelen aan een preregistratie van de koper van het ticket. Bij de toegangscontrole wordt geregistreerd wanneer de houder van het ticket het stadion is binnengekomen, inclusief zijn toegewezen zitplaats.

De veiligheidscoördinator stelt bij de analyse – door middel van een locatiesoftware van de slimme camera – vast dat de twee mannen zich bevonden op stoelnummer 15 (man 1) en 16 (man 2), vak D. Man 1 blijkt een seizoenkaarthouder te zijn. De veiligheidscoördinator stelt de identiteit van man 1 als volgt vast:

- aan de hand van de toegangspoortregistratie checkt de veiligheidscoördinator wie op stoel 15 is geregistreerd;
- de persoonsgegevens behorend bij stoel 15 zijn gekoppeld aan een seizoenskaart;
- Aangezien seizoenkaarthouders reeds een foto hebben moeten inleveren ten behoeve van de seizoenkaart, kan de veiligheidscoördinator de identiteit van man 1 vaststellen. De ingeleverde foto komt overeen met man 1 op de vastgelegde beelden tijdens de wedstrijd.

Man 2 is daarentegen geen seizoenkaarthouder. De identiteit van man 2 wordt als volgt vastgesteld:

- de veiligheidscoördinator stelt aan de hand van de preregistratie de naam en het adres vast van degene die op stoel 16 is geregistreerd;
- ook kan de veiligheidscoördinator vaststellen dat degene die op stoel 16 is geregistreerd om 14:30 uur door toegangspoort 3 het voetbalstadion is binnengekomen;
- de veiligheidscoördinator stelt aan de hand van de bewakingsbeelden op dat tijdstip van toegangspoort 3 vast dat degene die op stoel 16 is geregistreerd man 2 is.

Nu beide mannen zijn geïdentificeerd, komt daarmee de identificatiefase ten einde.

(zie bijlage 3 voor de volledige casus (signalering – identificatie – sanctie))

6.2.3 Fase 3 – Gebruik van de gegevens ten behoeve van sanctieoplegging

De door middel van de inzet van slimme technologie verkregen bewijsmiddelen kunnen vervolgens worden ingezet ten behoeve van het opleggen van een sanctie. Het slachtoffer, de voetbalclub, de KNVB en de politie respectievelijk het OM beschikken over de volgende mogelijkheden om een sanctie op te (laten) leggen voor discriminatoire of racistische gedragingen.

Zie bijlage 2 bij dit rapport voor een uitvergrote versie van de sanctiekaart.

Verdere verwerking

Het verstrekken van de beelden en geluidsopnamen en de bijbehorende gegevens door de BVO aan een derde partij (bijvoorbeeld aan een andere voetbalclub, de KNVB of de politie, de deskundigen of de behandelaren/beoordelaars respectievelijk de rechters van de zaak) ten behoeve van het opleggen van een sanctie betreft een verdere verwerking. Wij menen dat deze verwerking verenigbaar is met het oorspronkelijke doeleinde van de verzameling. Er is een duidelijk verband tussen de doeleinden waarvoor de gegevens zijn verzameld (de signalering, identificatie en/of het opleggen van een sanctie voor onrechtmatig gedrag) en het doeleinde van de verstrekking (de identificatie en/of het opleggen van een sanctie aan de potentiële dader/de betrokkene van de discriminerende of racistische uitlating).[85] Ook het kader waarbinnen de persoonsgegevens worden verzameld blijft grotendeels hetzelfde. Daarbij geldt bovendien dat het in de redelijke verwachting van de betrokkene ligt dat dergelijke beelden en andere gegevens met deze partners worden uitgewisseld ten behoeve van het opleggen van een sanctie aan de bij discriminatie of racisme betrokkenen. Hoewel de toets aan de verenigbaarheidscriteria in onze optiek positief uitvalt en aldus gesproken kan worden van een verenigbare verdere verwerking, wijzen wij partijen erop dat zich ook enkele omstandigheden voordoen die juist afdoen aan de verenigbaarheid. Het gaat hier om de verwerking van gevoelige gegevens, met potentiële verstrekkende nadelige gevolgen voor de betrokkene. Tegen deze achtergrond raden wij de BVO, KNVB, politie en justitie aan om passende technische en organisatorische waarborgen te treffen om de privacyinbreuk te minimaliseren. In deel 2 van dit rapport doen wij uitgebreide aanbevelingen voor de te treffen technische en organisatorische waarborgen.

Volledigheidshalve merken wij op dat de partner die de gegevens ontvangt een eigen grondslag moet hebben om de ontvangen gegevens te verwerken.

Wettelijke grondslag & noodzakelijkheid

Ervan uitgaande dat de BVO (en/of eventuele andere verwerkingsverantwoordelijken) de noodzaak van de in identificatie- en signaleringsfase gekozen slimme technologieën goed heeft onderbouwd, kunnen de daarmee verkregen beeld- en geluidsopnames en andere (identificatie)gegevens evenzeer worden gebruikt voor het uiteindelijke opleggen van een sanctie aan de desbetreffende persoon. Van belang daarbij is overigens wel dat het bewijs beperkt blijft tot de strikt noodzakelijke, toereikende en relevante beelden, geluiden en persoonsgegevens. Andere gegevens zullen zo veel mogelijk verwijderd moeten worden. Gezien de gevoeligheid van de gegevens en ter bescherming van de geïdentificeerde betrokkenen, dient de toegang tot deze informatie beperkt te zijn tot de strikt noodzakelijke personen. Ook indien de informatie via de KVV wordt gedeeld, dienen partijen dataminimalisatie in ogenschouw

[85] Artikel 6, vierde lid, aanhef en onder a, AVG.

te nemen. Er zou enkel tot verstrekking van dergelijke informatie mogen worden overgegaan voor zover naar verwachting op basis van de beelden daadwerkelijk tot het opleggen van een sanctie zal kunnen worden overgegaan (zie eerdere sanctiekaart). Enkel die partijen zouden moeten worden geautoriseerd die daadwerkelijk tot het opleggen van een sanctie overgaan.

Voor zover de beelden en persoonsgegevens worden verstrekt ten behoeve van strafrechtelijke afdoening aan de politie respectievelijk het OM is de AVG niet langer van toepassing. Na ontvangst van deze informatie is de Wpg respectievelijk de Wjsg van toepassing. Kort en goed mogen deze beelden worden verwerkt voor zover dat noodzakelijk is voor de uitvoering van de politietaak (in dit concrete geval de opsporing van discriminatie of racisme) en de (eventuele) daaropvolgende strafrechtelijke procedure.

Doorbrekingsgrond voor de verwerking van bijzondere & strafrechtelijke persoonsgegevens (verstrekking)

Evenals in de identificatiefase (paragraaf 6.2.2 van dit rapport) menen wij dat in de sanctiefase niet zonder meer biometrische persoonsgegevens kunnen worden verwerkt. De uitzonderingsgrond van artikel 29 UAVG (de verwerking van biometrische gegevens is noodzakelijk voor authenticatie of beveiliging) doet zich in deze fase überhaupt niet voor, aangezien in de sanctiefase dergelijke beveiligingsdoeleinden niet worden nagestreefd. Wij zien daarentegen wel een andere potentiële doorbrekingsgrond die zou kunnen worden ingeroepen in een regionale of landelijke procedure die door de BVO of de KNVB wordt ingesteld ten behoeve van het opleggen van een stadionverbod als bedoeld in artikel 10 van de algemene voorwaarden van de KNVB.

Bijzondere persoonsgegevens die rechtmatig in de identificatiefase zijn verwerkt (bijvoorbeeld omdat de beelden rasgegevens bevatten die (onvermijdelijk) zijn verwerkt voor de identificatie van de persoon)[86] mogen, evenals strafrechtelijke persoonsgegevens, verder worden verwerkt als bewijs ten behoeve van een civiele of strafrechtelijke procedure, mits er daadwerkelijk één van de in de sanctiekaart genoemde (rechts)middelen is ingezet en de verwerking van deze gegevens strikt noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering (zie artikel 22, tweede lid, aanhef en onder e, UAVG jo. artikel 32, aanhef en onder d, UAVG). Deze noodzaak kan worden aangenomen als de beelden strikt noodzakelijk zijn voor de bewijsvoering.

Wij benadrukken dat de bewijsmiddelen (met daarin bijzondere of strafrechtelijke persoonsgegevens) ook in het kader van de aangifte bij de politie mogen worden verstrekt. De wetgever onderkent dat de aangiftebevoegdheid van artikel 161 Sv een grondslag biedt voor het verstrekken van strafrechtelijke én bijzondere persoonsgegevens aan de politie. Dat veronderstelt echter dat er in dat concrete geval

[86] Artikel 25, aanhef en onder a, UAVG.

aanleiding wordt gezien om aangifte te doen, met het oog op opsporing en vervolging. De redenering daarbij is als volgt.

Hoewel dit niet expliciet wordt opgemerkt in de tekst van artikel 161 Sv, is goed verdedigbaar dat bij een aangifte strafrechtelijke gegevens kunnen worden verstrekt. Een aangifte heeft immers per definitie betrekking op een (vermeend) strafbaar feit. In zoverre is artikel 161 Sv een lidstatelijke bepaling als bedoeld in artikel 10 AVG.

De verwerking van bijzondere persoonsgegevens in de aangifte kan vervolgens worden gebaseerd op artikel 23, aanhef en onder c, UAVG dat bepaalt dat bijzondere persoonsgegevens (voor zover noodzakelijk) in aanvulling op strafrechtelijke persoonsgegevens mogen worden verwerkt.

De wetgever heeft voorgaande conclusie in de consultatieversie van de Verzamelwet gegevensbescherming onderschreven door in een nieuw onderdeel van artikel 23 van de UAVG op te nemen dat de verwerking van bijzondere persoonsgegevens is toegestaan indien "de verwerking noodzakelijk is voor het voldoen aan een bevel of vordering op grond van het Wetboek van Strafvordering, voor het doen van aangifte of klacht van strafbare feiten of voor het voldoen aan een wettelijke aangifteplicht."[87] In de toelichting op deze bepaling licht de wetgever toe dat met deze toevoeging 'buiten iedere twijfel' wordt gesteld dat een ieder bij het doen van aangifte gerechtigd is om daarbij (voor zover noodzakelijk) bijzondere persoonsgegevens te verwerken.[88]

Doorbrekingsgrond voor de verwerking van bijzondere & strafrechtelijke persoonsgegevens (gedurende een civiele of bestuursrechtelijke procedure)

Voor zover het een civielrechtelijke procedure betreft (bijv. ten behoeve van het opleggen van een stadionverbod door de KNVB) zien wij gedurende deze procedure een potentiële doorbrekingsgrond voor de verwerking van biometrische gegevens met het oog op het opleggen van een sanctie aan betrokkenen. Wij achten het goed denkbaar dat in het kader van een dergelijke procedure behoefte bestaat om de bewijswaarde van de beelden te verhogen, door bijvoorbeeld een deskundige een nader onderzoek te laten verrichten naar de vaststelling van het delict of de identificatie van de dader te valideren aan de hand van de beelden en geluidsopnamen. Hier kan bijvoorbeeld gedacht worden aan stemherkenning achteraf of analyse van de mondbewegingen met de geluidsfragmenten, zodat de identiteit van de dader (wie riep wat) kan worden vastgesteld op een wijze die de rechter of de KNVB in staat stelt om diegene te bestraffen. Dit kan een eigen deskundige van de voetbalclub zijn, maar ook een deskundige die door een rechter wordt aangewezen. De

87 Zie: https://www.internetconsultatie.nl/verzamelwetgegevensbescherming.

88 Zie de Memorie van toelichting bij consultatieversie van de Verzamelwet Gegevensbescherming, p. 9: "Om buiten iedere twijfel te stellen dat een ieder die aangifte doet (of klacht) gerechtigd is om daarbij, voor zover noodzakelijk voor het doen van die aangifte (of klacht), ook bijzondere categorieën persoonsgegevens te verwerken, wordt voorgesteld dat te expliciteren in artikel 23 van de UAVG. Dat zelfde geldt vanzelfsprekend als iemand om te kunnen voldoen aan een vordering van bij voorbeeld een opsporingsambtenaar, een officier van justitie of een rechter(-commissaris), dergelijke gegevens dient te verwerken. Het voorgestelde onderdeel van artikel 23 van de UAVG geldt zowel voor de bevoegdheid tot het doen van aangifte of klacht als voor de situaties waarin het Wetboek van Strafvordering of een sectorale wet de verplichting bevat tot het doen van aangifte."

biometrische analyse wordt in dit concrete geval ingezet om de bewijswaarde van de opnamen te verhogen. Wij menen dat voor deze concrete situatie mogelijk wél een doorbrekingsgrond als bedoeld in artikel 9, tweede lid, AVG zou kunnen bestaan voor de verwerking van biometrische gegevens, mits kan worden aangetoond dat het (ter identificatie van de betrokkene) strikt noodzakelijk is dat de deskundige een geautomatiseerde biometrische analyse verricht. Een dergelijk verwerking zou naar verwachting gebaseerd kunnen worden op artikel 22, aanhef en onder e, UAVG dat bepaalt dat bijzondere persoonsgegevens mogen worden verwerkt voor zover dat noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Om deze verwerkingsgrondslagen te kunnen inroepen, benadrukken wij evenwel dat de BVO of de KNVB in beginsel al een rechtsmiddel moet hebben ingesteld of procedure moet hebben gestart tegen de desbetreffende persoon. In de rechtspraak wordt ook aangenomen dat deze grondslag een basis kan vormen voor de verwerking van persoonsgegevens die nodig zijn om een volgende stap te kunnen zetten in het in rechte aanspreken van een derde.[89] Tegen deze achtergrond is goed verdedigbaar dat de BVO aan de KNVB of een daartoe aangewezen deskundige op het moment dat een rechtsmiddel wordt ingezet de bewijswaarde van de beelden verhoogt door middel van een biometrisch analyse of een analyse waarbij bijzondere persoonsgegevens worden verwerkt. De enkele loutere mogelijkheid dat de BVO of de KNVB een civiele procedure overweegt, is aldus onvoldoende.

Wij wijzen in dit verband naar de opinie van de EDPB, Richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679, (pag. 13 en 14), waarin de EDPB een nadere toelichting geeft op artikel 49, eerste lid, aanhef en onder e, AVG. Deze bepaling regelt de internationale doorgifte van persoonsgegevens ten behoeve van het instellen van een rechtsvordering. Hoewel het hier gaat om internationale rechtsvorderingen, is de uitleg van het begrip 'rechtsvordering' in gelijke zin toepasbaar op de nationale evenknie van deze bepaling:

> "Hier valt een waaier aan activiteiten onder, bijvoorbeeld, in het kader van een strafrechtelijk of administratief onderzoek in een derde land (bv. in verband met anti- trustwetgeving, corruptie, handel met voorkennis of gelijkaardige situaties), waarvoor de afwijking kan worden toegepast op een gegevensdoorgifte om zichzelf te verdedigen of om een vermindering of annulering van een boete te verkrijgen die bij wet wordt voorgeschreven, bijvoorbeeld in een anti- trustonderzoek. Gegevensdoorgiften voor officiële procedures voor bewijsgaring en -uitwisseling in civiele procedures kunnen eveneens onder deze afwijking vallen. De afwijking kan ook betrekking hebben op acties van de gegevensexporteur om procedures in een derde land in te stellen, bijvoorbeeld het aanspannen van een rechtszaak of het aanvragen van goedkeuring van een fusie. De afwijking kan niet worden gebruikt voor de rechtvaardiging van een doorgifte van persoonsgegevens op basis van de loutere mogelijkheid dat juridische of formele procedures in de toekomst mogelijk zouden kunnen zijn.

[89] Zie Rb. Den Haag 30 april 2020, ECLI:NL:RBDHA:2020:3980.

> De combinatie van de termen "rechtsvordering" en "procedure" houdt in dat de relevante procedure een rechtsgrond moet hebben, en dat er sprake moet zijn van een formeel, wettelijk bepaald proces maar niet dat het noodzakelijkerwijs moet gaan om een juridische of administratieve procedure ("of enige buitengerechtelijke procedure"). Aangezien een doorgifte in het kader van een procedure moet worden gedaan, moet er een nauw verband bestaan tussen een gegevensdoorgifte en een specifieke procedure met betrekking tot de desbetreffende situatie. De theoretische toepasbaarheid van een bepaald soort procedure zou niet toereikend zijn.” (onderstreping toegevoegd)

Voor zover de deskundige een beroep wil doen op bovenstaande uitzonderingsgrond voor de inzet van biometrie, wijzen wij op de volgende aandachtspunten om de strikte noodzaak en de privacy by design & default te borgen:

- Gebruik slechts slimme (biometrische) technologieën waarvoor in voldoende mate wetenschappelijk onderzoek bestaat over de effectiviteit van de technologie, evenals informatie over de validatie van het achterliggende algoritme en verificatie van de aan het algoritme ten grondslag liggende factoren. Uit deze informatie moet in ieder geval blijken welke stappen genomen zijn in de ontwikkeling en validatie van de indicatoren van de technologieën (en of en door wie deze zijn ge-peerreviewed), alsook welke statistische trainingsmodellen gebruikt zijn.

- Licht in een verantwoordingsdocument (waar mogelijk) toe hoe de analyse van de beelden en het geluid plaatsvindt en motiveer daarbij standaard wat daarvan de onderliggende variabelen zijn.

- Overweeg ook hier een evaluatieprotocol op te stellen, waarmee de BVO of de deskundige doorlopend kan bezien of het gebruik van de slimme technologie voldoende effectief is. Voor zover zich signalen voordoen dat de effectiviteit of de bewijswaarde van de bestaande videosystemen te wensen overlaat, kunnen deze evaluaties als grondslag dienen voor de keuze van meer ingrijpende slimme technologieën.

- Zorg ervoor dat − naast het enkele gebruik van de slimme technologieën − ook altijd steekproefsgewijs gedurende een wedstrijd handmatig mogelijke discriminerende uitlatingen worden geselecteerd. Op deze manier kan worden gecontroleerd of de slimme technologieën juist staan afgesteld. Bij eventuele discrepanties zou dit een aanleiding kunnen zijn dat de slimme technologie niet naar behoren functioneert of niet juist is afgesteld.

Wij benadrukken dat het voorgaande slechts geldt voor procedures van de KNVB of de BVO of een bestuursrechtelijke of civiele procedure bij de rechter. De uitzondering is met name bruikbaar voor het laten uitvoeren van een biometrische eigen analyse of analyse door een daartoe aangestelde deskundige nadat reeds een procedure door de

KNVB of de BVO is geïnitieerd. Het gaat hier uitdrukkelijk niet om de strafrechtelijke sanctionering. Het gebruik van de gegevens in de strafrechtelijke context wordt gereguleerd door het Wetboek van Strafvordering, de Wpg en de Wjsg.

Casus inzet slimme technologie - Sanctiefase

De KNVB besluit allereerst civielrechtelijk op te treden tegen de twee mannen. Het doel is met name het opleggen van een landelijk stadionverbod. Daarnaast doet de BVO aangifte bij de politie tegen beide vormen van racistisch gedrag. De getroffen speler besluit evenwel af te zien van het doen van aangifte. De speler dient geen klacht in en machtigt de BVO evenmin om namens hem aangifte te doen.

Civielrechtelijk optreden

Zoals volgt uit de sanctiekaart heeft de KNVB verschillende opties om de twee mannen civielrechtelijk aan te spreken. De KNVB standaardvoorwaarden, die door clubs bij de in artikel 1 onder f van die standaardvoorwaarden bedoelde voetbalwedstrijden van toepassing verklaard dienen te worden, spelen bij deze sanctieoplegging (zowel voor de clubs als voor de KNVB) een sleutelrol. In aanvulling daarop kunnen clubs zich bij het opleggen van sancties ook baseren op de rechten die zij ontlenen aan het feit dat zij eigenaar of huurder zijn van het stadion waarin zij spelen. Artikel 8.5 van de KNVB standaardvoorwaarden verbiedt (onder andere) gedrag dat als beledigend kan worden ervaren:

> "8.5 Het is verboden zich in het Stadion te gedragen op een wijze die anderen als provocerend, bedreigend of beledigend kunnen ervaren. […]."

Artikel 10 van de KNVB standaardvoorwaarden kent clubs en de KNVB vervolgens het recht toe bij overtreding van deze (of andere) bepaling(en) verschillende sancties op te leggen, waaronder onmiddellijke verwijdering uit het stadion, ongeldigverklaring van het toegangsbewijs, of – met inachtneming van de Richtlijn termijn stadionverbod - de oplegging van een (landelijk) stadionverbod.

Civielrechtelijk optreden (vervolg)
In aanvulling op de verbintenisrechtelijke sanctiemogelijkheden die de standaardvoorwaarden de KNVB en clubs toekennen, wijzen wij (omwille van de volledigheid) op de aanvullende mogelijkheid om, desgewenst, ook buiten de KNVB standaardvoorwaarden om civielrechtelijk tegen verspreiders van racistische en discriminatoire uitlatingen op te treden. Dat kan op basis van artikel 6:162 van het Burgerlijke Wetboek, op grond waarvan, anders dan het geval is bij de KNVB standaardvoorwaarden, ook de slachtoffers van discriminatoire of racistische uitingen zelf de mogelijkheid hebben in rechte tegen de verspreiders van die uitingen op te treden.

Het door de slimme technologie verzamelde bewijsmateriaal (signalering en identificatie van de daders) zal in het kader van de civielrechtelijke procedure als bewijs mogen worden ingebracht. Eventuele bijzondere en strafrechtelijke persoonsgegevens op de beelden (bijvoorbeeld de van de beelden af te lezen indirecte rasgegevens van beide mannen dat ten behoeve van identificatie is verwerkt) mogen ten behoeve van de procedure worden verstrekt, mits er daadwerkelijk één van de in de sanctiekaart genoemde (rechts)middelen is ingezet en de verwerking van deze gegevens strikt noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering (zie artikel 22, tweede lid, aanhef en onder e, UAVG jo. artikel 32, aanhef en onder d, UAVG). Deze noodzaak kan worden aangenomen als de beelden strikt noodzakelijk zijn voor de bewijsvoering.

Tijdens de procedure wordt door de KNVB vastgesteld dat op basis van het bestaande materiaal niet goed kan worden vastgesteld of man 2 zich schuldig maakt aan individuele belediging van de speler. De KNVB wijst een deskundige aan die door middel van een nadere analyse de bewijswaarde van de beelden of geluidsfragmenten poogt te verbeteren. Concreet krijgt deze deskundige de opdracht om vast te stellen of man 2 degene is die de individuele uiting heeft geroepen. Mits noodzakelijk voor de analyse, is het verdedigbaar dat daarbij bijzondere en/of strafrechtelijke persoonsgegevens worden verwerkt. De verwerking daarvan kan dan gebaseerd worden op artikel 22, tweede lid, aanhef en onder e, UAVG respectievelijk artikel 32, aanhef en onder d, UAVG. Er is immers één van de in de sanctiekaart genoemde (rechts)middelen ingezet en de verwerking van deze gegevens is strikt zijn voor de instelling, uitoefening of onderbouwing van een rechtsvordering. Op basis hiervan mogen dan ook biometrische gegevens worden verwerkt. De deskundige in deze zaak stelt na inzet van gezichtsherkenningstechnologie vast dat man 2 de individuele uiting heeft geroepen.

Uitkomst van de procedure is dat voor beide mannen een stadionverbod wordt opgelegd.

Strafrechtelijk optreden

Zoals eerder toegelicht, doet de BVO aangifte bij de politie tegen beide vormen van racistisch geweld. De getroffen speler besluit evenwel af te zien van het doen van aangifte. De speler dient geen klacht in en machtigt de BVO evenmin om namens hem aangifte te doen.

Zoals volgt uit de sanctiekaart kan de BVO aangifte doen voor groepsbelediging. De politie kan deze aangifte in behandeling nemen. Groepsbelediging (strafbaar gesteld in artikel 137c Wetboek van Strafrecht ('Sr')) betreft het zich in het openbaar opzettelijk beledigend uitlaten over een groep mensen, wegens onder meer hun ras. 'Ras' wordt ruim opgevat en betreft huidskleur, nationaliteit en etniciteit. Groepsbelediging is dus niet het beledigen van iemand *door* een groep, maar het beledigen door één of meer personen *van* een groep. 'Belediging' heeft de strekking een ander c.q. een groep bij het publiek in een ongunstig daglicht te stellen en in zijn eer of goede naam aan te tasten. Voor het bewijs van groepsbelediging is het niet vereist dat onder het publiek mensen aanwezig zijn van (bijvoorbeeld) joodse afkomst of met een donkere huidskleur. Het gaat erom dat de belediging publiekelijk is gehoord en gevoelens van vernedering of geschoktheid teweeg heeft kunnen brengen. Zie Hoge Raad 15 september 2009, ECLI:NL:HR:2009:BI4739, rov. 2.2.3.

De officier van justitie zal de rechtmatige (door middel van de slimme technologie vastgelegde) beelden met een beroep op Artikel 126nd Wetboek van Strafvordering ('Sv') kunnen vorderen bij de BVO. Artikel 126nd Sv bepaalt dat in geval van een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv de officier van justitie in het belang van het onderzoek van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens kan vorderen deze gegevens te verstrekken. Onder de misdrijven als bedoeld in artikel 67, eerste lid, Sv valt onder meer het misdrijf van artikel 137c Sr: *Hij die zich in het openbaar, mondeling (…) opzettelijk beledigend uitlaat over een groep mensen wegens hun ras (…) wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.*

De club die de camerabeelden heeft gemaakt van mogelijk strafbare gedragingen geldt als 'degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot vastgelegde gegevens' als bedoeld in artikel 126nd Sv. Aan de vordering van de officier van justitie dient te worden voldaan. Er is sprake van een wettelijke verplichting tot het verstrekken van persoonsgegevens (artikel 6, eerste lid, aanhef en onder c, AVG).

Strafrechtelijk optreden (vervolg)

Hoewel dit niet expliciet wordt opgemerkt in de aangiftebevoegdheid van artikel 161 Sv, is goed verdedigbaar dat de BVO bij de aangifte de beelden verstrekt met daarop strafrechtelijke gegevens. Een aangifte heeft immers per definitie betrekking op een (vermeend) strafbaar feit. In zoverre is artikel 161 Sv een lidstatelijke bepaling als bedoeld in artikel 10 AVG. De verwerking van bijzondere persoonsgegevens in de aangifte kan vervolgens worden gebaseerd op artikel 23, aanhef en onder c, UAVG dat bepaalt dat bijzondere persoonsgegevens (voor zover noodzakelijk) in aanvulling op strafrechtelijke persoonsgegevens mogen worden verwerkt.

Zodra de politie respectievelijk het OM de beelden hebben ontvangen, valt de verwerking van de daarin opgenomen persoonsgegevens niet langer onder de reikwijdte van de AVG. Vanaf dat moment is de Wpg respectievelijk de Wjsg van toepassing op de verwerking van de (bijzondere en/of strafrechtelijke) persoonsgegevens.

De rechter bepaalt vervolgens of de beelden toelaatbaar zijn als bewijs. De verwachting is dat de beelden als bewijsmateriaal zullen mogen worden gebruikt, voor zover de voetbalclub bij de inzet van de slimme technologie zich heeft gehouden aan de in dit rapport beschreven randvoorwaarden.

De politie kan de aangifte van de BVO gericht tegen de eenvoudige (individuele) belediging van de speler van de tegenpartij niet in behandeling nemen. Daarvoor is vereist dat het slachtoffer zelf aangifte doet of de BVO daarvoor volmachtigt. Aanvullend geldt dat het slachtoffer daadwerkelijk een klacht moet indienen (een klacht houdt in dat het slachtoffer expliciet verzoekt om vervolging). Doordat de speler dit niet heeft gedaan, kan de strafrechtelijke vervolging geen doorgang vinden. Het is de BVO niet toegestaan om de beelden en het dossier (incl. de daarin opgenomen strafrechtelijke en mogelijk zelfs bijzondere persoonsgegevens) aan de politie te verstrekken. Nu geen onderzoek mogelijk is, kan een dergelijke verstrekking niet noodzakelijk worden geacht. Daarmee eindigt de sanctiefase.

7 Geautomatiseerde besluitvorming en profilering

De AVG kent een strikt regime voor zogenoemde 'geautomatiseerde besluitvorming', waaronder profilering. Geautomatiseerde besluitvorming is in beginsel verboden, tenzij daarvoor een toereikende wettelijke grondslag bestaat (artikel 22 AVG). De vraag rijst of de inzet van de slimme technologieën in de signaleringsfase, identificatiefase of sanctioneringsfase zou leiden tot geautomatiseerde besluitvorming of profilering.

7.1 Juridisch kader

De AVG regelt dat bepaalde vormen van geautomatiseerde besluitvorming in beginsel verboden zijn. Artikel 22, eerste lid, AVG definieert een 'geautomatiseerd individueel besluit' als:

> "een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem aanzienlijke gevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft."

Profilering als bedoeld in art. 22, eerste lid, AVG vormt een bijzondere vorm van geautomatiseerde besluitvorming. Art. 4, aanhef en onder 4, AVG definieert 'profilering' als:

> "elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen".

De betrokkene hoeft geen specifieke actie te ondernemen om beschermd te worden tegen dergelijke besluitvorming.[90] Om te kunnen vaststellen of sprake is van geautomatiseerde besluitvorming als bedoeld in artikel 22 AVG dient te worden getoetst of sprake is van (i) een uitsluitend op geautomatiseerde verwerking gebaseerd besluit (ii) met rechtsgevolgen of dat de betrokkene anderszins in aanmerkelijke mate treft. Hieronder volgt een nadere uitwerking van deze begrippen.

[90] Zie Artikel-29 Werkgroep, Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, WP 251rev01, p. 23: "Dit verbod is van toepassing, ongeacht of de betrokkene wel of niet actie onderneemt met betrekking tot de verwerking van zijn persoonsgegevens. (…) Deze uitlegging versterkt het idee dat de betrokkene controle heeft over zijn persoonsgegevens, in overeenstemming met de grondbeginselen van de AVG. De uitlegging van artikel 22 als een verbod in plaats van een in te roepen recht houdt in dat personen automatisch beschermd zijn tegen de mogelijke gevolgen die dit soort verwerking kan hebben."

(i) Is sprake van een uitsluitend op geautomatiseerde verwerking gebaseerd besluit?

Een kernelement van geautomatiseerde besluitvorming is dat het besluit[91] uitsluitend met geautomatiseerde middelen moet zijn genomen, oftewel een besluit dat is genomen zonder menselijke tussenkomst in het besluitvormingsproces. Een geautomatiseerd proces dat slechts een aanbeveling doet (bijv. de aanbeveling dat een bepaalde werkwijze moet worden gevolgd), die vervolgens door een (veiligheids)medewerker van de BVO in combinatie met andere informatie wordt afgewogen bij het nemen van een uiteindelijk besluit, vormt geen geautomatiseerde besluit. Dergelijke op geautomatiseerde wijze voorbereide besluiten vallen niet onder de reikwijdte van artikel 22 AVG.

Hierbij zij benadrukt dat het inbouwen van enige vorm van menselijke tussenkomst er niet per definitie toe leidt dat geen sprake meer is van geautomatiseerde besluitvorming. De menselijke tussenkomst moet volgens de Artikel-29 Werkgroep zorgen voor zinvol toezicht op de besluitvorming. Het mag niet gaan o slechts een symbolische handeling, waarbij de beoordelaar de automatisch gegenereerde uitkomsten per definitie volgt. Daar komt bovendien bij dat degene die de menselijke tussenkomst uitvoert, bevoegd en bekwaam moet zijn om een andersluidend besluit te nemen. Tot slot geldt als voorwaarde dat hij alle relevante gegevens bij de herbeoordeling betrekt.[92]

(ii) Leidt het geautomatiseerde besluit tot rechtsgevolgen of is sprake van een besluit dat een betrokkene anderszins in aanmerkelijke mate treft?

Indien vastgesteld wordt dat inderdaad sprake is van een uitsluitend op geautomatiseerd verwerking gebaseerd besluit, dient vervolgens te worden gekeken naar de specifieke gevolgen van dat besluit. Het verbod van artikel 22 AVG is erop gericht om personen te beschermen tegen aanzienlijke effecten van geautomatiseerde besluitvorming. Zoals volgt uit de tekst van artikel 22 AVG is een geautomatiseerd besluit slechts verboden indien sprake is van 'besluitvorming met rechtsgevolgen' of 'besluitvorming die de betrokkene in aanmerkelijke mate treft'.[93]

Met besluiten waaraan rechtsgevolgen zijn verbonden, wordt volgens de Artikel 29-Werkgroep bedoeld een besluit dat van invloed is op iemands wettelijke rechten (zoals het stemrecht of het recht om rechtsmiddelen in te stellen). De Artikel 29-Werkgroep noemt als voorbeeld rechtsgevolgen die iemands juridische status of zijn rechten uit

---

91 De definitie van 'besluit' als bedoeld in de AVG is niet gelijk aan een besluit als bedoeld in artikel 1:3 Awb. Zie Kamerstukken II 2017/18, 34 851, nr. 3, p. 120: "Geautomatiseerde individuele besluitvorming is alleen aan de orde wanneer er sprake is van een besluit in de zin van de verordening. Dit begrip is niet slechts beperkt tot het besluitbegrip in de zin van de Awb, maar kan ook privaatrechtelijke rechtshandelingen betreffen."

92 Zie Artikel-29 Werkgroep, Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, WP 251rev01, p. 24.

93 Achterliggende gedachte van het verbod is dat "niemand mag worden onderworpen aan de gevolgen van een besluit enkel en alleen op basis van kenmerken van een bepaalde groep waartoe hij of zij behoort. De ratio van deze bepaling is dat het in dit licht bijzonder kwetsbaar is om besluitvorming te baseren op enkele persoonskenmerken" Vgl. Overweging 71 van de AVG en Kamerstukken II 2017/18, p. 39.

hoofde van een overeenkomst beïnvloeden, waaronder bijvoorbeeld: (i) het beëindigen van een overeenkomst, (ii) het recht op of weigering van een uitkering, zoals kinderbijslag of huurtoeslag of (iii) de weigering tot toelating tot een land of de toekenning van een nationaliteit.[94]

Betrekkelijk vager is de categorie besluiten die de betrokkene 'in aanmerkelijke mate treft'. Het gaat hier om besluiten die weliswaar geen rechtsgevolg teweegbrengen, maar de betrokkene toch in vergelijkbare mate kan treffen. De Artikel-29 Werkgroep neemt daarbij als uitgangspunt dat *"de effecten van de verwerking groot of belangrijk genoeg moeten zijn om aandacht te verdienen"*[95].

Het is moeilijk om in zijn algemeenheid te bepalen welk gevolg ernstig genoeg is om te kunnen spreken van een gevolg dat een betrokkene in aanmerkelijke mate treft. Een en ander zal moeten worden uitgekristalliseerd in de Europese en nationale rechtspraak. De Europese toezichthouders nemen als uitgangspunt dat sprake kan zijn van een besluit dat een betrokkene in aanmerkelijke mate treft indien het besluit het potentieel heeft om:[96]

> "[i] de omstandigheden, het gedrag of de keuzen van de betrokken personen in aanmerkelijke mate te treffen; [ii] een langdurig of blijvend effect op de betrokkene te hebben; of [iii] in het uiterste geval, tot uitsluiting of discriminatie van personen te leiden."

In de parlementaire geschiedenis van de (U)AVG en in de eerdergenoemde opinie van de Artikel-29 Werkgroep worden de volgende voorbeelden aangehaald:

- de automatische weigering van een (online) ingediende kredietaanvraag[97];
- verwerking van sollicitaties zonder menselijke tussenkomst[98];
- besluiten die iemands financiële situatie treffen, waaronder bijvoorbeeld het in aanmerking komen voor een lening[99];
- besluiten die iemands toegang tot gezondheidszorg treffen[100];
- besluiten waarmee iemand de toegang tot de arbeidsmarkt wordt geweigerd of waarmee hij ernstig wordt benadeeld;
- besluiten die iemands toegang tot onderwijs treffen, bijvoorbeeld de toelating tot een universiteit. [101]

---

94 Zie Artikel-29 Werkgroep, Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, WP 251rev01, p. 25.
95 Zie Artikel-29 Werkgroep, Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, WP 251rev01, p. 25.
96 Vgl. Artikel 29 Werkgroep, 'Guidelines on automateddecision-making and profiling', WP 251, p. 10-11.
97 Overweging 71 van de AVG.
98 Overweging 71 van de AVG.
99 Zie Kamerstukken II 2017/18, 34 851, nr. 3, p 26
100 Zie Kamerstukken II 2017/18, 34 851, nr. 3, p. 26
101 Vgl. Artikel 29 Werkgroep, 'Guidelines on automateddecision-making and profiling', WP 251, p. 10-11.

7.2 Aandachtspunten bij de inzet van slimme technologieën

Wij stellen voorop dat de inzet van slimme technologieën waarbij het gedrag van supporters (bijv. door middel van emotieherkenning) of de persoonlijke kenmerken van personen (door middel van biometrische identificatie) worden verwerkt, is aan te merken als profilering als bedoeld in artikel 4, aanhef en onder f, AVG. Ook de analyse van beelden en geluidsopnamen kan kwalificeren als profilering. Er worden dan aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijk persoon (geautomatiseerd) geëvalueerd (bijvoorbeeld het gedrag, de locatie en de verplaatsingen van supporters).[102] Voor zover het gedrag louter geautomatiseerd wordt geanalyseerd, is niet alleen sprake van 'profilering', maar ook van (in beginsel verboden) geautomatiseerde profilering als bedoeld in artikel 22, eerste lid, AVG.

Onzes inziens kan echter worden geoordeeld dat de inzet van slimme technologieën ten behoeve van de signalering, identificering en aanpak van discriminatie en racisme niet uitsluitend is gebaseerd op een louter geautomatiseerde verwerking. Van door de AVG verboden profilering is aldus in beginsel geen sprake. Daarbij is doorslaggevend dat bij de inzet van de beschreven slimme technologie de signalering en de identificatie weliswaar louter geautomatiseerd zou kunnen plaatsvinden, maar de daadwerkelijke sanctieoplegging (of dit nu door de voetbalclub, de KNVB of door justitie), en daarmee de besluitvorming, vooralsnog altijd door menselijke tussenkomst plaats zal vinden. De beelden en het geluid worden weliswaar geautomatiseerd gegenereerd en geselecteerd, maar worden nog altijd handmatig gecontroleerd. Bij de sanctieoplegging worden verschillende feiten en omstandigheden en de bewijswaarde van de beelden afgewogen. Kort en goed vormen de door de slimme technologieën gegenereerde (of eventueel geselecteerde) beelden enkel een onderbouwing voor het menselijke besluit of op basis van deze informatie voldoende grond bestaat om een sanctie op te leggen aan de desbetreffende persoon of personen.[103]

Naast het feit dat geen sprake is van louter geautomatiseerde verwerking, kan bovendien betwijfeld worden of de (eventuele) geautomatiseerde selectie in de signaleringsfase en de identificatiefase reeds tot gevolg heeft dat de betrokkene rechtsgevolgen ondervindt of sprake is van gevolgen die de betrokkene in aanmerkelijke mate treffen. Verdedigbaar is dat pas in de sanctiefase de betrokkene rechtsgevolgen respectievelijk aanmerkelijke gevolgen ondervindt van de (geautomatiseerde) selectie van zijn uitingen en beelden. Immers pas dan kan de betrokkene civiele of strafrechtelijke sancties opgelegd krijgen.

Wij wijzen erop dat het verdedigbare standpunt (dat de enkele geautomatiseerde selectie van incidenten en het geautomatiseerd identificeren van personen géén aanmerkelijke gevolgen heeft voor de betrokken persoon) zou kunnen leiden tot een juridische discussie. Gezien de afwezigheid van bestendige rechtspraak, is de kans

[102] Art. 4, aanhef en onder 4, AVG.
[103] Zie rechtbank Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1018, rov. 4.17 e.v.

aanwezig dat de rechter of de AP de inzet van slimme technologieën (waarbij risicogevallen geautomatiseerd worden geselecteerd met behulp van bijvoorbeeld emotieherkenning of geluidserkenning) *an sich* zal aanmerken als geautomatiseerde besluitvorming of profilering als bedoeld in artikel 22 AVG. De redenering daarbij zou zijn dat het enkele resultaat van de geautomatiseerde signalering en identificatie − los van de vraag of en zo ja, op welke wijze dat wordt betrokken bij de latere sanctieoplegging − reeds kan worden aangemerkt als een geautomatiseerd besluit met aanmerkelijke gevolgen voor de supporter.

> Relevant in dit verband is dat de Rechtbank Den Haag in haar uitspraak van 5 februari 2020 heeft laten doorschemeren dat enkel de geautomatiseerde selectie van een persoon waarbij (mogelijk) een verhoogde kans op sociale zekerheidsfraude bestaat, een 'aanmerkelijk gevolg' zou kunnen opleveren voor de geselecteerde persoon.[104] Het ging in deze uitspraak om de toepassing van het Systeem Risico Indicatie ('SyR**I'**), een geautomatiseerd systeem dat − kortgezegd − op basis van aangeleverde data een risicomelding doet over personen. Een risicomelding houdt in dat op basis van een vergelijking van (discrepanties in) bestanden is gebleken dat bij een persoon (mogelijk) een verhoogd risico bestaat op sociale zekerheidsfraude. Deze risicomelding mag vervolgens gedurende een periode van twee jaar door deelnemers van het SyRI-project worden gebruikt om een toezichtsonderzoek naar de betreffende persoon in te stellen. De rechtbank oordeelt op grond van artikel 8, tweede lid, EVRM dat de selectie als zodanig al een 'aanmerkelijk effect' kan hebben op de persoonlijke levenssfeer van de betrokkene.[105] Daarbij neemt de rechtbank in overweging dat een risicomelding twee jaar wordt opgeslagen en voor twintig maanden door deelnemers van het SyRI-project mag worden gebruikt. Hoewel de rechtbank een aanmerkelijk effect lijkt aan te nemen in de zin van artikel 8 EVRM (onder verwijzing naar een opinie van de Europese toezichthouders over geautomatiseerde besluitvorming als bedoeld in artikel 22 AVG), laat de rechtbank uitdrukkelijk in het midden of de selectie van een persoon c.q. de risicomelding voldoet aan de precieze definitie in de AVG van geautomatiseerde besluitvorming.

Evenwel heeft de inzet van slimme technologieën ter signalering en identificatie van discriminatie en racisme een duidelijk ondersteunend karakter. Deze inzet leidt op zichzelf, anders dan bijvoorbeeld het hiervoor besproken SyRI (waarbij het gevolg het instellen van een toezichtsonderzoek is), niet zonder meer tot een onderzoek of het

---

104 Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, rov. 6.59.

105 Artikel 8 EVRM regelt de bescherming van het recht op privéleven. Hoewel het recht op gegevensbescherming ontbreekt in de letterlijke tekst van artikel 8 EVRM, wordt in de rechtspraak van het Hof voor de Rechten van de Mens (hierna: EHRM) aangenomen dat ook gegevensbescherming onderdeel vormt van artikel 8 EVRM. Het EHRM gebruikt hiervoor de term 'gegevens die het privéleven raken'. De mate van bescherming van 'gegevens die het privéleven raken' is afhankelijk van de aard van de gegevens, de omvang van de gegevensverwerking, de wijze waarop de gegevens worden gebruikt, het doel van het gebruik, en de mogelijkheden die de verwerking biedt. De bescherming van artikel 8 EVRM is voorts niet absoluut en kan worden beperkt, mits wordt voldaan aan de uitzonderingsclausule van artikel 8, tweede lid, EVRM. De rechtbank heeft in geval van SyRI geoordeeld dat de geautomatiseerde selectie een aanmerkelijk effect heeft voor de betrokkene in de zin van artikel 8 EVRM, wat betekent dat moet worden voldaan aan eisen van artikel 8, tweede lid, EVRM. Hoewel deze eisen enigszins vergelijkbaar zijn met de AVG, dient de BVO en de KNVB zich ervan bewust te zijn dat sprake is van een ander regime. De AVG biedt vergelijkbare bescherming, maar is op aspecten strenger én concreter, zeker voor zover het gaat om geautomatiseerde besluitvorming.

opleggen van een sanctie. In zoverre behoeft de kans dat een rechter of de AP het standpunt inneemt dat sprake is van geautomatiseerde besluitvorming in de zin van artikel 22 AVG nuancering.

Hoewel gezien het voorgaande naar verwachting geen sprake is van een geautomatiseerd besluit of profilering, zoals bedoeld in artikel 22 AVG, brengen de overige vereisten van de (U)AVG, en met name het beginsel van rechtmatigheid, behoorlijkheid en transparantie,[106] met zich mee dat de inzet van de slimme technologieën wel voldoende inzichtelijk en controleerbaar moet zijn. De voetbalclub zal dus wel maatregelen moeten treffen om de transparantie van de slimme technologieën (en de achterliggende algoritmes) te borgen (zie hierover deel 2 van dit rapport).

[106] Artikel 5, eerste lid, aanhef en onder a, AVG.

DEEL 2

8 OVERIGE JURIDISICHE VOORWAARDEN VOOR DE INZET VAN SLIMME TECHNOLOGIEËN

8.1 Inleiding

In deel 1 van dit rapport hebben wij geconcludeerd dat wij het goed verdedigbaar achten dat BVO's een deel van de in hoofdstuk 3 beschreven slimme technologieën inzetten ten behoeve van het signaleren, identificeren en aanpakken van discriminatie, mits de BVO de strikte noodzaak en evenredigheid van de gekozen slimme technologie kan onderbouwen en verantwoorden. Wij hebben daarbij enkele aanbevelingen gedaan om de slimme technologieën in overeenstemming met de beginselen van privacy by design & default toe te passen. De AVG kent uiteraard nog meer randvoorwaarden waaraan (de verwerking van persoonsgegevens bij de inzet van) de slimme technologie moet voldoen. In dit deel lichten wij beknopt toe aan welke overige juridische (rand)voorwaarden iedere slimme technologie moet voldoen. Wij zullen daarbij concrete voorstellen doen voor de technische en organisatorische maatregelen die de verwerkingsverantwoordelijke partijen moet treffen om te voldoen aan de juridische voorwaarden van de AVG.

8.2 Internationale doorgifte

Indien persoonsgegevens worden verwerkt buiten de Europese Unie, is sprake van de internationale doorgifte van persoonsgegevens. Een dergelijke situatie doet zich bijvoorbeeld voor indien de BVO in het kader van de inzet van de slimme technologie of de opslag van de beelden gebruik zou maken van een Amerikaanse cloudopslagprovider die op buitenlandse servers ten behoeve van de BVO persoonsgegevens verwerkt. Een ander voorbeeld is dat de BVO de beelden en geluidsopnamen verstrekt aan een voetbalclub buiten de EU.

Uitgangspunt is dat de verwerkingsverantwoordelijke (zoals een BVO) in beginsel dient te voorkomen dat persoonsgegevens in het buitenland worden verwerkt. Mocht internationale doorgifte om specifieke redenen toch noodzakelijk zijn, dan dient de verwerkingsverantwoordelijke na te gaan of de doorgifte aan de buitenlandse verwerkingsverantwoordelijken, (sub)verwerkers of andere ontvangers in derde landen of internationale organisaties is toegestaan.

Bij naleving van de algemene verplichtingen uit de AVG kunnen persoonsgegevens binnen de EU vrij circuleren. Voor doorgifte buiten de EU aan zogenaamde derde landen of internationale organisaties gelden aanvullende verplichtingen op grond van hoofdstuk V van de AVG. Van doorgifte is ook sprake indien het ter beschikking stellen van gegevens plaatsvindt aan een (sub)verwerker die is gevestigd in een derde land.

Van belang is vooral dat doorgifte aan verwerkingsverantwoordelijken, verwerkers of andere ontvangers in derde landen of internationale organisaties niet ten koste gaat van het beschermingsniveau dat de AVG verzekert.

Doorgifte aan derde landen en internationale organisaties mag in ieder geval alleen plaatsvinden in overeenstemming met de AVG. Onder de AVG zijn de belangrijkste eventuele grondslagen voor de verwerkingsverantwoordelijke:

- het sluiten van een modelcontract[107] dat de Europese Commissie heeft opgesteld voor de verstrekking van persoonsgegevens aan een bewerker in een derde land[108];
- het sluiten van een modelcontract dat de AP heeft opgesteld en dat de EC heeft goedgekeurd;
- een goedgekeurde gedragscode of goedgekeurd certificeringsmechanisme, samen met bindende en afdwingbare toezeggingen om de passende waarborgen toe te passen;
- noodzakelijkheid vanwege gewichtige redenen van algemeen belang.[109]

De betrokkene moet worden geïnformeerd over het voornemen om persoonsgegevens door te geven aan derde landen of internationale organisaties (zie artikel 14, eerste lid, onderdeel f, AVG).

Aanbevelingen

- Gezien de gevoeligheid van de beelden en geluidsopnamen, raden wij aan om waar mogelijk internationale doorgifte aan derde landen te voorkomen. Dat geldt in het bijzonder bij het implementeren van cloudoplossingen.

- In het geval van doorgifte van persoonsgegevens aan derde landen, zal hetzelfde hoge beveiligingsniveau als in de AVG moeten worden gegarandeerd.

Een bijzonder aandachtspunt in dit kader is nog dat het Hof van Justitie bij uitspraak van 16 juli 2010 in de zaak C-311/18 (Schrems II) het zogenoemde 'Privacy Shield' ongeldig verklaard. Dit betekent dat de doorgifte van persoonsgegevens aan Amerikaanse verwerkers niet langer gebaseerd kan worden op dit adequaatheidsbesluit.

8.3 Rechtmatige, behoorlijke en transparante verwerking & non-discriminatiebeginsel

De verwerkingsverantwoordelijke dient op grond van de AVG te borgen dat persoonsgegevens behoorlijk en rechtmatig worden verwerkt.

Juridisch kader

[107] In de AVG aangeduid als 'standaardbepalingen'.
[108] Zie voor deze modelcontracten: https://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.
[109] Zie voor meer informatie de art. 45 t/m 49 AVG.

Artikel 5, eerste lid, aanhef en onder a, AVG schrijft voor dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Dit beginsel vindt zijn uitwerking in een groot deel van de overige privacyeisen die uit de AVG volgen. Zo komt het beginsel van transparantie onder meer tot uiting in de informatieplichten die op verwerkingsverantwoordelijken rusten (zie daarover paragraaf 9.2 hierna).

Voor wat betreft dit beginsel is in de context van de inzet van slimme technologieën in voetbalstadions evenwel het volgende relevant. Een reëel risico bij de inzet van slimme technologie, waarbij gebruik wordt gemaakt van een algoritme (met name emotieherkenning of biometrie (waaronder gezichtsherkenning)), is dat het onderliggende algoritme (onbedoeld) zou kunnen leiden tot directe of indirecte discriminatie van toeschouwers. Het recht op non-discriminatie vereist dat gelijkwaardige personen door de slimme technologie gelijkwaardig worden geselecteerd, ongeacht leeftijd, ras of geslacht. Een benadeling van specifieke personen en groepen is alleen aanvaardbaar als daarvoor een objectieve en redelijke rechtvaardiging bestaat. De inzet van een slimme technologie mag niet leiden tot ongerechtvaardigd (indirect) onderscheid, bijvoorbeeld omdat deze enkel geluidsopnamen maakt van overtreders van een bepaalde etniciteit. Voor zover dat wel het geval is, dient de verwerking 'onbehoorlijk' te worden geacht, wat een overtreding betreft van artikel 5, eerste lid, aanhef en onder a, AVG.

De AP is recentelijk in een onderzoeksrapport naar de verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag[110] ('Onderzoeksrapport') zeer uitgebreid ingegaan op het discriminatieverbod. De AP hanteert daarin het volgende juridische kader:

> "Het beginsel van behoorlijkheid betekent in ieder geval dat verwerkingen niet in strijd mogen zijn met fundamentele rechtsbeginselen, zoals het discriminatieverbod. Het discriminatieverbod ligt ten grondslag aan de volgende bepalingen. Op grond van artikel 26 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (hierna: IVBPR) zijn allen gelijk voor de wet en hebben zonder discriminatie aanspraak op gelijke bescherming door de wet. In dit verband verbiedt de wet discriminatie van welke aard ook en garandeert een ieder gelijke en doelmatige bescherming tegen discriminatie op welke grond ook, zoals ras, huidskleur, geslacht, taal, godsdienst, politieke of andere overtuiging, nationale of maatschappelijke afkomst, eigendom, geboorte of andere status.
>
> Op grond van artikel 1, eerste lid, van Protocol nr. 12 bij het Verdrag tot bescherming van de rechten van de mens en fundamentele vrijheden (hierna: EVRM) moet het genot van elk in de wet neergelegd recht worden verzekerd zonder enige discriminatie op welke grond dan ook, zoals geslacht, ras, kleur, taal, godsdienst, politieke of andere mening, nationale of

[110] Onderzoeksrapport AP 'Belastingdienst/Toeslagen – De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag' van 17 juli 2020, z2018-22445 (raadpleegbaar via: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_belastingdienst_kinderopvangtoeslag.pdf).

maatschappelijke afkomst, het behoren tot een nationale minderheid, vermogen, geboorte of andere status. Ingevolge het tweede lid van die bepaling mag niemand worden gediscrimineerd door enig openbaar gezag op met name een van de in het eerste lid vermelde gronden.

Op grond van artikel 1 van de Grondwet worden allen die zich in Nederland bevinden, in gelijke gevallen gelijk behandeld. Discriminatie wegens godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht of op welke grond dan ook, is niet toegestaan. Op grond van artikel 1, eerste lid, van het Internationaal Verdrag inzake de uitbanning van alle vormen van rassendiscriminatie wordt elke vorm van onderscheid, uitsluiting, beperking of voorkeur op grond van ras, huidskleur, afkomst of nationale of etnische afstamming die ten doel heeft de erkenning, het genot of de uitoefening, op voet van gelijkheid, van de rechten van de mens en de fundamentele vrijheden op politiek, economisch, sociaal of cultureel gebied, of op andere terreinen van het openbare leven, teniet te doen of aan te tasten, dan wel de tenietdoening of aantasting daarvan ten gevolge heeft, niet toegestaan.

Bij de beoordeling of sprake is van discriminatie, is van belang dat niet is vereist dat zich twee in alle opzichten gelijke gevallen voordoen. Van belang is of de betrokken gevallen in relevante opzichten voldoende vergelijkbaar zijn.[111] Verder staat het discriminatieverbod niet in de weg aan iedere ongelijke behandeling van in relevante opzichten gelijke gevallen, maar slechts aan die behandeling die als ongerechtvaardigd onderscheid moet worden beschouwd, omdat voor het gemaakte onderscheid geen redelijke en objectieve rechtvaardiging bestaat. Dit doet zich voor indien dat onderscheid geen legitiem doel dient of er geen redelijke, proportionele verhouding is tussen de gebruikte middelen en het doel dat daarmee wordt beoogd te realiseren.[112] Dit toetsingskader is gelijkelijk van toepassing op artikel 26 van het IVBPR[113] en artikel 1 van Protocol nr. 12 bij het EVRM[114] en artikel 1 van de Grondwet.[115]"

Om te bepalen of de verwerkingen van de variabelen of de werking van de slimme technologie en het daaraan ten grondslag liggende algoritme is aan te merken als discriminerende verwerkingen, hanteert de AP de volgende cumulatieve criteria:[116]

"1. de tegenover elkaar gestelde gevallen zijn in relevante opzichten voldoende vergelijkbaar;
2. er is onderscheid gemaakt tussen deze gevallen;
3. het onderscheid heeft tot nadeel geleid in behandeling;

111 Par. 56 van het arrest van het EHRM van 13 december 2011 (Ludana tegen Slowakije, ECLI:CE:ECHR:2011:1213JUD003182702).
112 Par. 125 van het arrest van het EHRM van 22 maart 2012 (Konstantin Markin tegen Rusland, ECLI:CE:ECHR:2012:0322JUD003007806) en par. 90 van het arrest van het EHRM van 25 maart 2014, (Biao tegen Denemarken, ECLI:CE:ECHR:2016:0524JUD003859010)
113 Vergelijk ow. 2.4 van de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 30 maart 2016 (ECLI:NL:RVS:2016:865).
114 Vergelijk ow. 2.5.2 van het arrest van de Hoge Raad van 13 april 2018 (ECLI:NL:HR:2018:429).
115 Vergelijk ow. 3.4.2 van het arrest van de Hoge Raad van 8 oktober 2004 (ECLI:NL:HR:2004:AP0424) en ow. 2.4.1 van het arrest van 4 november 2016 (ECLI:NL:HR:2016:2495). Onderzoeksrapport | z2018-22445 49
116 Onderzoeksrapport AP 'Belastingdienst/Toeslagen – De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag' van 17 juli 2020, z2018-22445, p. 47 e.v.

> 4. het onderscheid is niet redelijk en objectief gerechtvaardigd, omdat het geen legitiem doel dient en/of er geen redelijke en proportionele verhouding bestaat tussen het onderscheid en het daarmee beoogde doel."

Verschil in behandeling op basis van een verdachte grond is enkel toegelaten als daarvoor zeer zwaarwegende redenen ("*very weighty reasons*") bestaan.[117] De bewijslast voor de redelijke en objectieve rechtvaardiging voor het maken van onderscheid op basis van een verdachte grond ligt bij de verwerkingsverantwoordelijke.[118] Dit volgt overigens ook uit de verantwoordingsplicht van de verwerkingsverantwoordelijke in de zin van artikel 5, tweede lid, van de AVG.[119]

Beoordeling

Er bestaat een risico dat bij de inzet van slimme technologieën − met name de slimme technologieën waarbij beelden en opnamen geautomatiseerd worden gemaakt en/of geanalyseerd door een algoritme − onbedoeld verboden onderscheid wordt gemaakt op leeftijd, geslacht of ras/etniciteit. Zonder strikte waarborgen in zowel het ontwikkelproces als de toepassing van de technologie, kan dergelijke discriminatie onbedoeld tot vertekende resultaten leiden. Daarbij kan gedacht worden aan het relatief vaker selecteren van personen van een specifieke etnische afkomst, terwijl ook andere personen dezelfde uitlatingen doen in het stadion. Een ander aspect is het feit dat met name bij gezichtsherkenningssoftware leeftijd, geslacht en raciale afkomst de nauwkeurigheid van de meeste algoritmes beïnvloeden en daarmee kunnen afdoen aan de goede werking van de slimme technologie.

Los van de verwerkingsverantwoordelijkheid van de partij die de slimme technologie inzet, vervult de ontwikkelaar van de aan de slimme technologie ten grondslag liggende algoritmes een sleutelrol bij het voorkomen van onbedoeld verboden onderscheid. De ontwikkelaar zou daarbij onderstaande risicofactoren voor het ontstaan van discriminatie bij toepassing van algoritmes in acht kunnen nemen:

> Het risico op discriminatie bij de toepassing van algoritmes kan door een combinatie van factoren ontstaan. Reeds in 2011 hebben onderzoekers Barocas en Selbst vijf factoren geïdentificeerd die er (onbedoeld) toe kunnen leiden dat een (door middel van machine learning ontwikkeld) algoritme disproportionele nadelige gevolgen oplevert voor bepaalde bevolkingsgroepen in de samenleving.[120]

---

[117] Par. 87 van het arrest van 18 februari 2009, (Andrejeva tegen Letland, ECLI:NL:XX:2009:BI1815), zie ook CRvB, 5 juni 2018, ECLI:NL:CRVB:2018:1541, USZ 2017/332 met annotatie van M.W. Venderbos.

[118] Par. 92 van het arrest van het EHRM van 25 maart 2014, (Biao tegen Denemarken, ECLI:CE:ECHR:2016:0524JUD003859010).

[119] Onderzoeksrapport AP 'Belastingdienst/Toeslagen − De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag' van 17 juli 2020, z2018-22445, p. 47 e.v.

[120] Barocas, Solon and Selbst, Andrew D., Big Data's Disparate Impact (2016). 104 California Law Review 671 (2016), Available at SSRN: https://ssrn.com/abstract=2477899 or http://dx.doi.org/10.2139/ssrn.2477899.

Factor 1 – Het vaststellen van de doelvariabelen (‘**target variables’**) en de klassenlabels (‘class labels’)
Indien bij de ontwikkeling van het algoritme machine-learning wordt toegepast, wordt er door middel van analyses statistische verbanden gezocht in de dataset. Deze analyse is niet geheel objectief, maar wordt beïnvloed door de formulering van de gewenste uitkomst (‘doelvariabele’). De doelvariabele zal moeten worden omgezet naar een programmeerbare probleemstelling. In aanvulling daarop worden de eigenschappen van de gewenste uitkomst verdeeld in categorieën, zogenoemde ‘klassenlabels’. Het vaststellen van de doelvariabele en de daaraan ten grondslag liggende klassenlabels is een subjectief proces. Het is goed mogelijk dat de datascientist zich (onbedoeld) laat leiden door een bias bij het vaststellen van de programmeerbare probleemstelling en de klassenlabels.

Factor 2 - De kwaliteit van de trainingsdata
Een tweede factor die kan leiden tot onbedoelde discriminatie is de kwaliteit van de trainingsdataset. De kwaliteit, waarde en objectiviteit van de data in de dataset is bepalend voor de objectiviteit van de voorspellingen van het algoritme. Indien de trainingsdataset van slechte kwaliteit is (bijvoorbeeld omdat sprake is van een slecht geselecteerde testgroep), zal het algoritme onjuiste voorspellingen doen die onbetrouwbaar of discriminerend zijn (‘**garbage in, garbage out’**). Kort en goed kunnen zich twee problemen voordoen met betrekking tot de betrouwbaarheid van de dataset.

Ten eerste bestaat het risico dat dat de dataset het product is van beslissingen gebaseerd op vooroordelen (‘**labelling examples’**) met als gevolg dat het algoritme deze vooroordelen zal reproduceren.

Ten tweede kan de onzorgvuldige selectie van een niet-representatieve dataset - oftewel het selecteren van een dataset met een duidelijke over- of ondervertegenwoordiging – eveneens leiden tot discriminatoire voorspellingen. Dergelijke onbetrouwbare voorspellingen kunnen onder meer ontstaan door ‘overfitting’. Daarmee wordt bedoeld dat het algoritme te veel gestoeld is op de unieke kenmerken van de specifieke dataset. Indien het model vervolgens wordt toegepast op een andere dataset verliest het model zijn voorspellende kracht. Door te werken met een testset wordt overfitting opgespoord, doordat bij het toepassen van het model op de testset zal blijken dat de voorspellende waarde verdwijnt bij een andere dataset.

Factor 3 - Feature selection
Ook het toepassen van ‘feature selection’ kan onbedoeld leiden tot discriminatoire gevolgen. De selectie van de variabelen waaruit het algoritme zal bestaan wordt (mede) bepaald door de subjectieve overtuigingen van de data-scientist. Het is van belang dat bij de toepassing van feature selection enkel objectieve variabelen worden geselecteerd. Er dient zoveel mogelijk voorkomen te worden dat variabelen worden geselecteerd die direct of indirect verband houden met een specifieke bevolkingsgroep. Ook het selecteren van variabelen die (in)direct verband houden met bijzondere persoonsgeven als bedoeld in art. 9, eerste lid, AVG, zal naar waarschijnlijkheid leiden tot discriminatoire uitkomsten.

Factor 4 - Proxies

Een vierde factor die kan leiden tot onbedoelde discriminatie is dat het model, óók na het verwijderen van bijzondere persoonsgegevens uit de dataset, schijnbaar objectieve variabelen bevat die proxies zijn voor beschermde kenmerken. Dergelijke proxies reflecteren vaak maatschappelijke ongelijkheden en zijn in beginsel onwenselijk. Het gebruik van dergelijke proxies leidt tot schending van het wettelijke non-discriminatiebeginsel, indien de keuze voor de betreffende variabele niet uitlegbaar of te rechtvaardigden is.

Factor 5 – Maskeren
Tot slot is het mogelijk dat de hiervoor beschreven vier factoren van discriminatie welbewust kunnen worden ingezet om te verhullen dat het algoritme leidt tot discriminatoire uitkomsten ('masking').

Technische en organisatorische waarborgen

- Stel voorafgaand aan de ontwikkeling van het algoritme een strategie of een protocol vast om te voorkomen dat ongerechtvaardigde vertekening wordt gecreëerd of versterkt. Daarbij dient oog te zijn voor zowel de inputgegevens als het ontwerp van het algoritme.

- Zorg voor een klachtmechanisme waardoor het voor betrokkenen en derden mogelijk wordt om vertekening, discriminatie of slechte prestaties van het algoritme te melden. Zorg in aanvulling daarop voor een protocol waarin wordt beschreven op welke wijze dergelijke klachten in behandeling zullen worden genomen. Neem een verwijzing naar dit protocol op in de onderlinge regeling wanneer er sprake is van gezamenlijke verwerkingsverantwoordelijkheid ten aanzien van (het algoritme behorende bij) de betreffende slimme technologie. Dit klachtenmechanisme is erop gericht om de juistheid, behoorlijkheid en rechtmatigheid van de inzet van de aan de slimme technologie ten grondslag liggende algoritme te borgen. Deze klachtmogelijkheid dient onderscheiden te worden van het recht op bezwaar als beschreven in artikel 21 van de AVG. Dit recht kan worden ingeroepen om toekomstige, doorlopende verwerkingen te staken.

- Laat voorafgaand aan de toepassing van het algoritme en de slimme technologie een onafhankelijke audit verrichten naar de mogelijke bias en discriminatoire effecten van het algoritme (zogenoemde 'discrimination testing'), bijvoorbeeld door de software en de code van het algoritme te laten toetsen door een technisch specialist.

- Test en monitor potentiële vertekeningen gedurende de toepassingsfase.

- Creëer bewustzijn bij de medewerkers van BVO'S en/of andere verwerkingsverantwoordelijken die de slimme technologie ontwikkelen of toepassen over de wijze waarop een bias kan ontstaan, welke gevolgen dit heeft en hoe dergelijke bias kan worden voorkomen.

8.4 Juistheidsbeginsel

In artikel 5, eerste lid, aanhef en onder d, AVG is het beginsel van juistheid van de gegevens geformuleerd. Verwerkingsverantwoordelijken moeten op grond van artikel 5, eerste lid, aanhef en onder d, AVG alle redelijke maatregelen nemen om persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

De verwerkingsverantwoordelijke kan niet (zonder meer) uitgaan van de juistheid van de geluidsopnamen en beeldopnamen, en is zelf verantwoordelijk voor de controle en het waarborgen van de juistheid, integriteit en actualiteit van de verwerkte gegevens en opnamen. De verwerkingsverantwoordelijke moet op grond van de AVG de nodige maatregelen treffen om ervoor te zorgen dat de persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn.

Technische en organisatorische maatregelen

- Bouw altijd een menselijk controlemoment in waarbij wordt gecontroleerd of de koppeling van de beelden en de geluidsopnamen en de vaststelling van de identiteit van de betrokkene juist heeft plaatsgevonden.

- Geef een indicatie van de mate van (on)zekerheid van de kwaliteit en juistheid van de gemaakte beeld- en geluidopnamen.[121] Licht bovendien toe wat de mate van (on)zekerheid bepaalt.

- Ontwerp een 'terugmeld-mechanisme', zodat eventuele in de ontwikkeling of toepassing van het algoritme en de slimme technologie vastgestelde onjuistheden of gebreken kunnen worden hersteld.

- Stel een periodiek controleproces vast dat (i) borgt dat fouten of vooroordelen in de verzamelde of gedeelde gegevens en (ii) fouten of vooroordelen in het algoritme worden opgemerkt. Stel daarbij concreet vast welke persoon of welke partij dit controleproces uitvoert.

- Voer steekproefsgewijs een controle uit om te beoordelen of de aan de slimme technologieën ten grondslag liggende algoritmen voldoende nauwkeurig zijn. Voorkom daarmee overmatig vertrouwen in de uitkomsten van het algoritme en de slimme technologie. Daarbij kan gedacht worden aan een maatregel waarbij naast de door het algoritme geselecteerde incidenten ook altijd ter controle andere incidenten worden geselecteerd en beoordeeld. Indien blijkt dat deze incidenten wél hadden moeten worden geselecteerd

[121] Bijvoorbeeld: de voorspelling dat de gefilmde persoon ook degene is die de racistische leus heeft uitgesproken is voor 89% zeker.

door het algoritme, dan kan dit aanleiding vormen voor het bijstellen van het algoritme.

- Hanteer passende wiskundige en statistische procedures waarmee factoren die aanleiding geven tot onjuistheden van persoonsgegevens worden gecorrigeerd en het risico op fouten wordt geminimaliseerd.

8.5 Beginsel van opslagbeperking

Artikel 5, eerste lid, aanhef en onder e, AVG bepaalt dat persoonsgegevens in een vorm die het mogelijk maakt de betrokkenen te identificeren niet langer worden bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.

> Persoonsgegevens die voor verwijdering of vernietiging in aanmerking komen kunnen met het oog op archivering voor het algemeen belang, historische, statistische of wetenschappelijk doeleinden overeenkomstig artikel 89, eerste lid, AVG worden bewaard (zie tevens artikel 5, eerste lid, aanhef en onder e, AVG). Daarbij geldt wel dat de verwerking dient te voldoen aan de voorwaarden die voor statistisch of wetenschappelijk onderzoek gelden én passende technische en organisatorische maatregelen moeten worden getroffen om de rechten en vrijheden van de betrokkene te beschermen.

In diverse sectorale wetten worden specifieke bewaartermijnen genoemd. Deze specifieke bewaartermijnen gaan voor op voornoemde algemene bepaling over het bewaren van persoonsgegevens in de AVG.

Het voorgaande maakt dat de BVO's, de KNVB en andere ontvangers strikte bewaartermijnen moeten formuleren voor de door slimme technologie vervaardigde beeld- en geluidsopnamen. Dat geldt ook voor andere persoonsgegevens die deze partijen verkrijgen, bijvoorbeeld in het kader van preregistratie.

8.6 Beveiliging

De verwerkingsverantwoordelijke is op grond van de AVG verplicht tot het treffen van passende beveiligingsmaatregelen die de veiligheid en vertrouwelijkheid van de persoonsgegevens borgt die gedurende de toepassing van het algoritme worden verwerkt. De AVG bevat minimale beveiligingseisen waaraan de verwerkingsverantwoordelijke zich tijdens de ontwikkeling en toepassing van een slimme technologie dient te houden.

Juridisch kader

Artikel 5, eerste lid, aanhef en onder f, AVG bepaalt dat een verwerkingsverantwoordelijke door het nemen van passende technische en organisatorische maatregelen een passende beveiliging van persoonsgegevens dient te

waarborgen, zodat de persoonsgegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Daarbij moet de verwerkingsverantwoordelijke, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te kunnen waarborgen.[122] Bij de beoordeling van het passende beveiligingsniveau dient met name rekening te worden gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens, hetzij per ongeluk hetzij onrechtmatig. Waar passend, omvatten de beveiligingsmaatregelen onder meer het volgende:

> a) de pseudonimisering en versleuteling van persoonsgegevens;
> b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
> c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
> d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.[123]

De hierboven beschreven algemene beveiligingsplicht maakt dat de verwerkingsverantwoordelijke verplicht is om te waarborgen dat de persoonsgegevens die worden verwerkt als gevolg van de inzet van slimme technologie voldoende zijn beveiligd. Bovendien moet de verwerkingsverantwoordelijke erop toezien dat de getroffen beveiligingsmaatregelen ook daadwerkelijk worden nageleefd. Het gaat het bestek van dit rapport te buiten om in detail te bespreken aan welke technische vereisten de beveiliging in de ontwikkelingsfase en toepassingsfase dient te voldoen. Bij het vaststellen van de beveiligingsmaatregelen zou aansluiting kunnen worden gezocht bij de Richtsnoeren Beveiliging van persoonsgegevens van de AP.[124]

Technische en organisatorische maatregelen

- Stel een beveiligingsplan vast dat concreet is toegespitst op de toepassing van de slimme technologie en de daarmee geselecteerde beelden en geluidsopnamen, ga daarbij meer concreet in op de volgende aspecten:

[122] Artikel 32 AVG.
[123] Artikel 32, eerste lid, AVG.
[124] https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidregels_beveiliging_van_persoonsgegevens.pdf.

- het verhinderen dat onbevoegden toegang krijgen tot apparatuur voor de verwerking;
- het verhinderen dat onbevoegden gegevensdragers lezen, kopiëren, wijzigen of verwijderen;
- het verhinderen dat onbevoegden gegevens invoeren of opgeslagen gegevens inzien, wijzigen of verwijderen;
- het verhinderen dat onbevoegden systemen voor geautomatiseerde gegevensverwerking gebruiken met behulp van datatransmissieapparatuur;
- de maatregelen die ervoor zorgen dat personen die geautoriseerd zijn om het systeem voor geautomatiseerde gegevensverwerking te gebruiken, uitsluitend toegang hebben tot de gegevens waarop hun autorisatie betrekking heeft;
- de maatregelen die ervoor zorgen dat kan worden nagegaan en vastgesteld aan welke partijen gegevens zijn verstrekt of beschikbaar gesteld met behulp van datatransmissieapparatuur;
- maatregelen die ervoor zorgen dat later kan worden nagegaan en vastgesteld welke gegevens wanneer en door wie in een systeem voor geautomatiseerde gegevensverwerking zijn ingevoerd;
- maatregelen die verhinderen dat onbevoegden gegevens lezen, kopiëren, wijzigen of verwijderen tijdens de doorgifte van die gegevens of het vervoer van gegevensdragers;
- maatregelen die ervoor zorgen dat de geïnstalleerde systemen in geval van storing opnieuw kunnen worden ingezet.

- Toets periodiek de hierboven beschreven beveiligingsmaatregelen. Houd daarbij rekening met de stand van de techniek. Actualiseer voor zover nodig de beveiligingsmaatregelen.

- Waarborg – conform het hierboven genoemde beveiligingsplan – door middel van een autorisatiematrix en een controleproces dat degenen die toegang verkrijgen tot de omgeving van de slimme technologie, de geselecteerde geluidsopnamen en beelden en/of andere verkregen persoonsgegevens daadwerkelijk daartoe bevoegd zijn.

- Maak (met de gezamenlijke verwerkingsverantwoordelijken) heldere afspraken over het verrichten van audits en het geven van uitvoering aan de resultaten van beveiligingsaudits.

- Stel technische en organisatorische maatregelen vast (waaronder een noodplan) om eventuele schade te beperken in het geval een beveiligingsgebrek wordt geconstateerd.

- Waarborg dat eventuele (sub)verwerkers eveneens passende beveiligingsmaatregelen treffen.

8.7 De verantwoordingsplicht

De verwerkingsverantwoordelijke voor (verwerking van persoonsgegevens met) de slimme technologie moet onder de AVG verantwoorden dat hij de beginselen en voorwaarden van de AVG naleeft. Dit volgt uit de in art. 5, tweede lid, AVG opgenomen 'verantwoordingsplicht'.

Art. 24, eerste lid, AVG bepaalt in het verlengde daarvan dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen neemt om te waarborgen en te kunnen aantonen dat de verwerkingen, in dit geval de verwerkingen die gepaard gaan met de inzet van de slimme technologie, in overeenstemming met de AVG worden uitgevoerd. Een van die maatregelen kan zijn dat de verwerkingsverantwoordelijke gegevensbeschermingsbeleid opstelt en uitvoert (artikel 24, tweede lid, AVG). Bij de vraag of en zo ja, welke maatregelen moeten worden genomen, houdt de verwerkingsverantwoordelijke rekening met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen. De maatregelen moeten worden geëvalueerd en indien nodig geactualiseerd. Een van de manieren om (deels) uitvoering te geven aan voorgaande eisen betreft het bijhouden van een verwerkingsregister (artikel 30 AVG).

Technische en organisatorische maatregelen

- Stel een privacybeleid op waarin specifiek wordt ingegaan op de wijze waarop persoonsgegevens wordt verwerkt ten behoeve van de toepassing van de slimme technologie.

- Werk dit privacybeleid zo nodig uit in concrete privacy protocollen, zodat de medewerkers die de slimme technologie toepassen en/of de daarmee verkregen beeld-en geluidsopnamen en/of andere persoonsgegevens ontvangen op de hoogte zijn van de concrete stappen die zij moeten zetten om de privacy van betrokkenen te waarborgen.

- Neem in het verwerkingsregister een beschrijving op van de verwerkingen die plaatsvinden in het kader van de toepassing van de slimme technologie.

8.8 De meldplicht datalekken

De verwerkingsverantwoordelijken zullen bij eventuele datalekken[125] in specifieke gevallen verplicht zijn om deze te melden aan de AP en de betrokkenen.

[125] In de AVG wordt gesproken over een inbreuk in verband met persoonsgegevens. Dat is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (artikel 4 aanhef en onder 12 AVG). Er wordt gemakshalve gesproken van datalek.

Artikel 33 van de AVG ziet op de melding van een datalek aan de AP. Een datalek moet altijd gemeld worden, tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De melding moet zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat duidelijk is geworden dat sprake is van datalek, worden gedaan. Als dat niet lukt, moet in de melding worden gemotiveerd waarom dat zo is. Als het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan dat ook in stappen (zonder onredelijke vertraging).

Op grond van het vijfde lid van artikel 33 AVG moeten alle inbreuken worden gedocumenteerd (inclusief feiten, gevolgen en getroffen rectificerende maatregelen). De documentatie moet de AP in staat stellen de naleving van artikel 33 van de AVG te controleren.

Artikel 34 van de AVG bevat de verplichting om een inbreuk te melden aan de betrokkene als deze "waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen". De melding moet onverwijld worden gedaan.

8.9 Data Protection Impact Assessment (DPIA)

Op grond van artikel 35 van de AVG moet de verwerkingsverantwoordelijke een DPIA uitvoeren als een soort verwerking – in het bijzonder een waarbij nieuwe technologieën worden gebruikt – gelet op de aard en de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

De Europese privacy toezichthouders hebben criteria opgesteld om het risico van een verwerking te bepalen.[126] Daarnaast heeft de AP (conform artikel 35, vierde en vijfde lid, AVG) een lijst op haar website gepubliceerd van verwerkingen waarvoor een DPIA verplicht is. De AP schrijft (onder meer) een DPIA voor bij cameratoezicht, profilering, observatie en de inzet van biometrie. Uit de door de AP geformuleerde criteria volgt dat voor de beoogde toepassingen van slimme technologieën een DPIA zal moeten worden verricht.

Een DPIA moet ten minste de volgende onderdelen bevatten:

- een systematische beschrijving van de beoogde verwerkingen, de doelen van de verwerking en, in voorkomend geval, de gerechtvaardigde belangen die door de inzet van de slimme technologie worden behartigd;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
- de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming

[126] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dDPIA#in-welke-gevallen-moet-ik-een-dDPIA-uitvoeren-5879

van persoonsgegevens te garanderen en om aan te tonen dat aan de AVG is voldaan.

Is de uitkomst van de DPIA dat de met de inzet van de slimme technologie gepaard gaande verwerking een hoog risico zou opleveren als de BVO, de KNVB en/of een andere verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken[127], dan moet de verwerkingsverantwoordelijke (in de persoon van de functionaris voor gegevensbescherming) de AP voorafgaand aan de verwerking raadplegen. Daarbij moet de informatie worden verstrekt die is genoemd in het derde lid van artikel 36 van de AVG (waaronder de DPIA, de doelen en middelen van de voorgenomen verwerking en de maatregelen en waarborgen die zullen worden getroffen respectievelijk geboden). Indien de AP van oordeel is dat de voorgenomen verwerking een inbreuk op de AVG zou maken, dan geeft de AP − in beginsel binnen acht weken − een schriftelijk advies aan de verwerkingsverantwoordelijke. Ook mag de AP dan haar in artikel 58 van de AVG opgenomen bevoegdheden uitoefenen.

Bij het wijzigen van de met de verwerking gepaarde risico's dient opnieuw te worden beoordeeld of de verwerking overeenkomstig de DPIA wordt uitgevoerd (artikel 35, elfde lid, AVG).

[127] In overweging 94 van de AVG is nog toegevoegd 'en de verwerkingsverantwoordelijke van mening is dat het niet mogelijk is dat risico te beperken door middel van maatregelen die met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn'. Het is niet duidelijk of daadwerkelijk van deze (op het oog logische) inperking moet worden uitgegaan, nu die niet in art. 36 AVG is opgenomen.

9 TRANSPARANTIE EN RECHTEN VAN BETROKKENEN

9.1 Inleiding

De verwerkingsverantwoordelijke partijen zullen ook (aanvullende) technische en organisatorische maatregelen moeten treffen om de uitoefening van de rechten van de betrokkene mogelijk te maken. Het gaat daarbij om:

- het recht op informatie (artikelen 13 en 14 AVG);
- het recht op inzage (artikel 15 AVG);
- het recht op rectificatie (artikel 16 AVG);
- het recht op wissing (artikel 17 AVG);[128]
- het recht op beperking van de verwerking (artikel 18 AVG);
- het recht op dataportabiliteit (artikel 20 AVG); en tot slot
- het recht op bezwaar (artikel 21 AVG).

In dit deel zal worden besproken of bovengenoemde rechten specifieke privacy issues met zich meebrengen in de context van de inzet van slimme technologie in voetbalstadions en zo ja, welke maatregelen getroffen zouden kunnen worden om de uitoefening van deze rechten in die context zo goed mogelijk te faciliteren.

Op alle hierboven genoemde rechten kan een uitzondering worden gemaakt. Soms gaat het daarbij om specifieke bij het recht behorende uitzonderingen. Voor zover dat het geval is, komen die bij de bespreking van het betreffende recht aan bod. Er zijn ook uitzonderingen die voor alle genoemde rechten gelden. Die uitzonderingen worden aan het einde van dit deel besproken (paragraaf 9.9).

Tot slot zij hier nog opgemerkt dat de verwerkingsverantwoordelijke partijen onverwijld en in ieder geval binnen een maand na ontvangst daarvan, gevolg moet geven aan verzoeken van betrokkenen die zijn gebaseerd op de artikelen 15 t/m 21 AVG. Bij complexe verzoeken of een groot aantal verzoeken kan deze termijn met twee maanden worden verlengd (artikel 12, derde lid, AVG). Als de verwerkingsverantwoordelijke partij het verzoek afwijst, moet hij onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek aan de betrokkene meedelen waarom het verzoek zonder gevolg is gebleven (artikel 12, vierde lid, AVG). De verwerkingsverantwoordelijke partij moet, alvorens een beslissing op het verzoek te nemen, zorgen voor een deugdelijke vaststelling van de identiteit van de verzoeker als over die identiteit twijfels zouden bestaan (artikel 12, zesde lid, AVG).

9.2 Het recht op informatie

Op grond van artikel 13 en 14 AVG moet, tenzij sprake is van een uitzonderingsgrond, de verwerkingsverantwoordelijke de betrokkene informeren over:

[128] Het recht op wissing wordt ook wel aangeduid als het recht op vergetelheid.

- diens identiteit en contactgegevens en, indien aan de orde, van zijn vertegenwoordiger;
- de doelen waarvoor de persoonsgegevens worden verwerkt en de rechtsgrond van de verwerking;
- (indien aan de orde) het gerechtvaardigd belang op grond waarvan de verwerking is gebaseerd;
- de (categorieën van) ontvangers[129];
- eventuele doorgifte van persoonsgegevens aan een derde land of een internationale organisatie[130];
- de bewaartermijn;
- de rechten van de betrokkene;
- of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
- als de verwerking op toestemming is gebaseerd: dat de betrokkene het recht heeft de verleende toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan; en
- het bestaan van geautomatiseerde besluitvorming en nuttige informatie over de onderliggende logica, alsmede het belang en de te verwachte gevolgen van die verwerking voor de betrokkene.

Als de persoonsgegevens niet van de betrokkene zijn verkregen, moet de verwerkingsverantwoordelijke de betrokkene ook informeren over:

- de betrokken categorieën van persoonsgegevens; en
- de bron van de informatie en, in voorkomend geval, of dit een openbare bron is.

Voorts bevelen wij aan dat de betrokkenen ook worden geïnformeerd over de werking van de slimme technologie als zodanig (zie daarover ook hoofdstuk 7 over geautomatiseerde besluitvorming).

---

129 De term 'ontvanger' is gedefinieerd in artikel 4, aanhef en onder 9, van de AVG: "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt". Daaronder vallen volgens de Artikel 29-Werkgroep onder meer: andere verwerkingsverantwoordelijken, gezamenlijke verwerkingsverantwoordelijken en verwerkers aan wie/waaraan gegevens worden doorgegeven of verstrekt. Hoewel dit volgens de Artikel 29-Werkgroep wel de voorkeur verdient, is het niet noodzakelijk om de ontvangers bij naam te noemen. Een verwerkingsverantwoordelijke kan volstaan met het noemen van de categorieën van ontvangers. De informatie over de ontvangers dient zo specifiek mogelijk te zijn door aanduiding van het type ontvangers (oftewel door vermelding van de activiteiten die die ontvangers verrichten) en de industrie, de sector, de subsector en de locatie van de ontvangers. Vgl. Artikel-29 Werkgroep, 'Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679', WP260 rev.01, p. 43.

130 En ook aanvullende informatie hierover, zie de artikelen 13 en 14 AVG.

Op grond van artikel 12 AVG moet de verwerkingsverantwoordelijke passende maatregelen nemen opdat de betrokkene bovenstaande informatie in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm verkrijgt en in duidelijke en eenvoudige taal. In de praktijk wordt de informatie vaak gegeven door middel van een schriftelijke privacyverklaring die fysiek of elektronisch aan de betrokkene wordt verstrekt.

Er zijn verschillende situaties waarin niet hoeft te worden geïnformeerd, namelijk als:

- de betrokkene al op de hoogte is van de informatie die anders verstrekt zou worden[131];
- het verstrekken van de informatie onmogelijk[132] blijkt of een onevenredige inspanning[133] zou vergen (deze uitzonderingsgrond geldt alleen als de gegevens *niet* bij de betrokkene zijn verkregen)[134];
- het voldoen aan de informatieverplichting de doelen van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen (deze uitzonderingsgrond geldt alleen als de gegevens *niet* bij de betrokkene zijn verkregen)[135];
- de vastlegging/verkrijging/verstrekking van de persoonsgegevens in nationaal of Europees recht is voorgeschreven en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen (deze uitzondering geldt alleen als de gegevens *niet* bij de betrokkene zijn verkregen);
- de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim (deze uitzondering geldt alleen als de gegevens *niet* bij de betrokkene zijn verkregen);
- zich een situatie voordoet als bedoeld in artikel 23 AVG jo. artikel 41 UAVG (zie paragraaf 9.9).

Bovengenoemde informatieverplichting leidt in beginsel niet tot specifieke privacyrechtelijke issues in de context van de inzet van slimme technologie in voetbalstadions. Net als iedere andere verwerking die buiten die context plaatsvindt, zullen de betrokkenen overeenkomstig artikelen 13 en 14 AVG moeten worden geïnformeerd over de verwerking van persoonsgegevens rondom voetbalwedstrijden.

---

131 Zie artikel 13, vierde lid, AVG en artikel 14, vijfde lid, aanhef en onder a, AVG.

132 Het verstrekken van informatie is volgens de Artikel-29 Werkgroep pas onmogelijk indien de verwerkingsverantwoordelijke kan aantonen "welke factoren hem of haar feitelijk verhinderen om de informatie in kwestie aan de betrokkene te verstrekken. (...) In de praktijk zullen er zeer weinig situaties zijn waarin een verwerkingsverantwoordelijke kan aantonen dat het feitelijk onmogelijk is om de informatie aan betrokkenen te verstrekken." Vgl. Artikel-29 Werkgroep, 'Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679', WP260 rev.01, p. 34.

133 Uit Overweging 62 van de AVG volgt dat bij de beoordeling van de 'onevenredige inspanning' in aanmerking mag worden genomen om hoeveel betrokkenen het gaat, hoe oud de gegevens zijn en welke passende waarborgen worden ingebouwd. Vgl. Artikel-29 Werkgroep, 'Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679', WP260 rev.01, p. 35-36.

134 In dat geval moeten passende maatregelen worden genomen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie.

135 Zie daarover ook Artikel-29 Werkgroep, 'Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679', WP260 rev.01, p. 37: "Om gebruik te kunnen maken van deze uitzondering moeten verwerkingsverantwoordelijken aantonen dat de verstrekking van de informatie van artikel 14, eerste lid, op zichzelf al de verwezenlijking van de doeleinden van die verwerking zou frustreren."

Het verdient aanbeveling om maatregelen te treffen die borgen dat de privacyverklaring (en eventuele wijzigingen in de inhoud daarvan) tijdig – en bij voorkeur geautomatiseerd – aan de betrokkene wordt verstrekt, bijvoorbeeld voorafgaand aan de aanschaf van een toegangskaart.

Voorts is van belang dat de BVO's en de KNVB, voor zover zij als gezamenlijke verwerkingsverantwoordelijkheden optreden, in een onderlinge regeling vaststellen hoe uitvoering wordt gegeven aan de informatieverplichting, en deze onderlinge regeling ter beschikking stellen aan betrokkenen.

Technische en organisatorische waarborgen

- Zorg dat voorafgaand aan de inzet van slimme technologie waaraan een algoritme ten grondslag ligt er altijd een externe audit is verricht van de technische werking en juistheid van het model (en een eventuele bias) en overweeg om deze uitkomsten op de website van de BVO of de KNVB beschikbaar te stellen (incl. de datum en uitslag van deze technische audit), tenzij zich daar reden toe verzetten. Archiveer de overwegingen waarom het beschikbaar stellen van de algemene toelichting op het algoritme niet wenselijk is.

- Overweeg om op de eigen website van de BVO of de KNVB een pagina in te richten waarop algemene informatie kan worden opgenomen over:
  - het doel van de slimme technologie
  - de wijze waarop de slimme technologie is ontwikkeld en toegepast.

- Stel een privacyverklaring op die voldoet aan de vereisten van art. 14 AVG, tenzij sprake is van een wettelijke uitzondering op de informatieverplichting.

- (Verplicht bij art. 14 AVG en voor zover sprake is van gezamenlijke verwerkingsverantwoordelijkheid) Maak heldere afspraken met de gezamenlijke verwerkingsverantwoordelijke(n) over de inhoud van de privacyverklaring, de wijze van het beschikbaar stellen daarvan en de procedure voor het wijzigen en actualiseren van de privacyverklaring. Neem deze afspraken vervolgens op in de onderlinge regeling die de gezamenlijke verwerkingsverantwoordelijken op grond van art. 26, eerste lid, AVG moeten opstellen. Het opstellen van een onderlinge regeling is onder de Wjsg niet verplicht.

- Verstrek bij de toepassing van slimme technologie waarbij gebruik wordt gemaakt van een onderliggend algoritme nuttige informatie over de wijze van totstandkoming van het model, de validatie van het risicomodel en de verificatie van de risico-indicatoren. Deze informatie kan worden verstrekt op het moment dat de uitkomst met de betrokkene wordt gedeeld of na een bezwaar of verzoek om inzage van de betrokkene.

- Informeer de betrokkene over de methoden die door de BVO of de KNVB worden gebruikt om doorlopend te toetsen of de slimme technologie eerlijk, doelgericht en onbevooroordeeld blijft.

9.3 Het recht op inzage

De verwerkingsverantwoordelijke partijen zullen maatregelen moeten treffen om de uitoefening van het recht op inzage van de betrokkene mogelijk te maken. De betrokkene heeft op grond van artikel 15 AVG het recht om van een verwerkingsverantwoordelijke partij kosteloos uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens met de slimme technologie en, wanneer zijn gegevens worden verwerkt, het recht op inzage in die persoonsgegevens. De verwerkingsverantwoordelijke partij moet in dat geval een kopie van de persoonsgegevens aan de betrokkene verstrekken en de volgende informatie verschaffen:

- de verwerkingsdoeleinden;
- de betrokken categorieën van persoonsgegevens;
- de (categorieën van) ontvangers;
- de bewaartermijn die wordt gehanteerd of, als dat niet mogelijk is, de criteria om die termijn te bepalen;
- de rechten van de betrokkenen;
- alle beschikbare informatie over de bron van de persoonsgegevens als deze niet bij de betrokkene zijn verkregen;
- het bestaan van geautomatiseerde besluitvorming en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Bij toepassing van slimme technologie in voetbalstadions moeten de verwerkingsverantwoordelijke partijen kunnen voldoen aan inzageverzoeken. Voor de hand ligt dat iedere partij voor dat deel waarvoor zij verantwoordelijk is, zorgdraagt voor het behandelen van inzageverzoeken. Zo zou de KNVB bijvoorbeeld inzage kunnen bieden in de persoonsgegevens die zij verwerkt uit de KVV en, in het verlengde daarvan, bij de procedure tot oplegging van een stadionverbod. De BVO zou inzage kunnen bieden in de met slimme technologie vastgelegde en anderszins verwerkte persoonsgegevens. Daarbij wijzen wij erop dat de met slimme technologie gemaakte opnames (in fase 1) slechts beperkt mogen worden opgeslagen, namelijk slechts voor de duur dat het noodzakelijk is om de opnames te bewaren (zie paragraaf 6.2). In opnames die zijn vernietigd kan logischerwijs geen inzage meer worden geboden.

De verwerkingsverantwoordelijke partijen kunnen − of, in het geval van gezamenlijke verwerkingsverantwoordelijkheid; moeten − afspraken maken over de wijze waarop

uitvoering wordt gegeven aan het inzagerecht en aan de andere rechten van betrokkenen (zie paragraaf 9.4 tot en met 9.8) in de praktijk. In die afspraken kan dan worden vastgelegd tot wie de betrokkenen zich kunnen wenden indien zij hun rechten willen uitoefenen.

De Wpg en de Wjsg bevatten een eigen regime over de uitoefening van de rechten van betrokkenen ten aanzien van politiegegevens respectievelijk justitiële en strafvorderlijke gegevens.[136]

9.4 Het recht op rectificatie

De betrokkene heeft op grond van artikel 16 AVG recht op rectificatie van onjuiste persoonsgegevens die een verwerkingsverantwoordelijke over hem verwerkt. Daarnaast heeft hij het recht op vervollediging van onvolledige persoonsgegevens. Een en ander voor zover zich geen weigeringsgrond voordoet.

9.5 Het recht op gegevenswissing

Op grond van artikel 17, eerste lid, AVG heeft de betrokkene recht op wissing van hem betreffende persoonsgegevens. De verwerkingsverantwoordelijke partij is bij ontvangst van een dergelijk verzoek verplicht persoonsgegevens te wissen indien zich één van de volgende situaties voordoet:

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- (als de verwerking op toestemming is gebaseerd en er is geen andere rechtsgrond voor de verwerking): de betrokkene trekt zijn toestemming in;
- de persoonsgegevens zijn onrechtmatig (bijvoorbeeld in strijd met artikel 5 AVG) verwerkt;
- de betrokkene maakt conform artikel 21 AVG bezwaar tegen een verwerking gebaseerd op artikel 6, eerste lid, aanhef en onder e of onder f, AVG en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking[137];
- de persoonsgegevens moeten worden gewist om te voldoen aan een in het Unierecht of het lidstatelijk recht neergelegde verplichting die op de verwerkingsverantwoordelijke rust;
- de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.

Als de verwerkingsverantwoordelijke partij bij de inzet van de slimme technologie de persoonsgegevens die moeten worden gewist (eerder) openbaar heeft gemaakt, moet

[136] Zie artikel 24a Wpg e.v. en artikel 17a Wjsg e.v.
[137] Zie voor een bespreking van het recht op bezwaar paragraaf 9.8.

hij op grond van artikel 17, tweede lid, AVG redelijke maatregelen (waaronder technische maatregelen) treffen om andere verwerkingsverantwoordelijken die de persoonsgegevens (ook) verwerken ervan op de hoogte te stellen dat de betrokkene heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen. Bij het nemen van die maatregelen mag de verwerkingsverantwoordelijke rekening houden met de beschikbare technologie en de uitvoeringskosten.

Artikel 17, derde lid, AVG bevat uitzonderingsgronden op de in het eerste lid opgenomen verplichting om persoonsgegevens te wissen. Een verwerkingsverantwoordelijke is onder meer niet verplicht persoonsgegevens te wissen voor zover de verwerking van die persoonsgegevens nodig is:

i. voor het nakomen van een in het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust;
ii. voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;
iii. om redenen van algemeen belang op het gebied van volksgezondheid overeenkomstig artikel 9, tweede lid, aanhef en onder h en i, AVG en artikel 9, derde lid, AVG (zie paragraaf 6.4 van dit rapport);
iv. met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, voor zover wissing de verwezenlijking van de doelen van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen.

9.6 Het recht op beperking van de verwerking

De betrokkene heeft op grond van artikel 18, eerste lid, AVG het recht op beperking van de verwerking van zijn persoonsgegevens. Beperking van de verwerking houdt in dat persoonsgegevens slechts mogen worden verwerkt, met uitzondering van de opslag ervan, met toestemming van de betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering door de betrokkene of ter bescherming van de rechten van een ander natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Unie of voor een lidstaat.

De verwerkingsverantwoordelijke moet overgaan tot het beperken van de verwerking indien een van de volgende situaties van toepassing is:

a) de juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt de juistheid van de persoonsgegevens te controleren;
b) de verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;

c) de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
d) de betrokkene heeft overeenkomstig artikel 21, eerste lid, bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.

9.7 Het recht op dataportabiliteit

De verwerkingsverantwoordelijke partijen zullen op grond van artikel 20 AVG maatregelen moeten treffen zodat betrokkenen hun recht op overdraagbaarheid (ook wel het recht op dataportabiliteit) uit kunnen oefenen ten aanzien van hun persoonsgegevens die worden verwerkt met de slimme technologie. Het recht op overdraagbaarheid van gegevens verplicht verwerkingsverantwoordelijke partijen om een technische mogelijkheid te creëren om de persoonsgegevens in een gestructureerd, algemeen gebruikt en machinaal leesbaar formaat (zoals PDF) te kunnen verstrekken. De betrokkene heeft dit recht alleen als:

- de verwerking berust op toestemming (artikel 6, eerste lid, aanhef en onder a, AVG / artikel 9, eerste lid, aanhef en onder a AVG) of op een overeenkomst (artikel 6, eerste lid, aanhef en onder b, AVG); en
- de verwerking via geautomatiseerde procedés wordt verricht.

Dit recht lijkt voor wat betreft de inzet van slimme technologieën niet relevant, aangezien de inzet van deze technologieën is gebaseerd op het gerechtvaardigde belang om racisme en discriminatie te signaleren, identificeren en aan te pakken (artikel 6, eerste lid, aanhef en onder f, AVG).

9.8 Het recht op bezwaar

Als de persoonsgegevens bij inzet van de slimme technologie worden verwerkt op grond van artikel 6, eerste lid, aanhef onder e en f, AVG, kan de betrokkene daartegen op grond van artikel 21, eerste lid, AVG bij de verwerkingsverantwoordelijke partij te allen tijde bezwaar maken vanwege met zijn specifieke situatie verband houdende redenen. De voor de verwerking verantwoordelijke partij staakt vervolgens de verwerking van de persoonsgegevens, tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

Deze eis leidt niet tot specifieke issues in de context van de inzet van slimme technologie in voetbalstadions.

9.9 Uitzonderingen op de rechten van de betrokkene

Op grond van artikel 23 AVG kunnen uitzonderingen worden gemaakt op de rechten van betrokkenen (waaronder begrepen de informatieplicht). Deze uitzonderingen zijn uitgewerkt in artikel 41, eerste lid, UAVG:

> 1. De verwerkingsverantwoordelijke kan de verplichtingen en rechten, bedoeld in de artikelen 12 tot en met 21 en artikel 34[138] van de verordening, buiten toepassing laten voor zover zulks noodzakelijk en evenredig is ter waarborging van:
> a. de nationale veiligheid;
> b. landsverdediging;
> c. de openbare veiligheid;
> d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
> e. andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
> f. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
> g. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
> h. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g;
> i. de bescherming van de betrokkene of van de rechten en vrijheden van anderen[139]; of
> j. de inning van civielrechtelijke vorderingen.

De verwerkingsverantwoordelijke partij zal zelf moeten afwegen of zich een of meer uitzonderingsgronden voordoen. Daarbij moet hij op grond van artikel 41, tweede lid, UAVG in ieder geval, voor zover van toepassing, rekening houden met:

> a. de doeleinden van de verwerking of van de categorieën van verwerking;
> b. de categorieën van persoonsgegevens;
> c. het toepassingsgebied van de ingevoerde beperkingen;
> d. de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte;

[138] Dit artikel ziet op de plicht om bepaalde datalekken aan de betrokkene te melden.
[139] Onder "anderen" kan ook de verwerkingsverantwoordelijke worden begrepen.

e. de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
f. de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking;
g. de risico's voor de rechten en vrijheden van de betrokkenen; en
h. het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.

Tot slot wordt benadrukt dat ook de sectorale wetgeving specifieke uitzonderingsgronden kan bevatten.

Disclaimer

Dit onderzoeksrapport is opgesteld voor en in opdracht van het ministerie van VWS. Anderen dan het ministerie kunnen aan dit onderzoeksrapport geen rechten ontlenen. Op dit rapport zijn de algemene voorwaarden van Pels Rijcken & Droogleever Fortuijn N.V. van toepassing, te raadplegen via https://www.pelsrijcken.nl/algemene-voorwaarden.

Bijlage 1

Randvoorwaarden voor statistisch onderzoek ten behoeve van de training en statistische analyse werking slimme technologie.

Randvoorwaarden statistisch onderzoek

Om in het kader van de ontwikkeling van een algoritme een beroep te kunnen doen op de statistische onderzoeksexceptie is noodzakelijk dat wordt voldaan aan de strikte randvoorwaarden die de UAVG aan een statistisch onderzoek stelt (artikel 89 AVG jo. artikel 24 UAVG). Het is in dit licht aldus allereerst van belang dat de ontwikkelingsfase zo is ingericht dat een beroep kan worden gedaan op de statistische onderzoeksexceptie. Hieronder volgt een nadere toelichting van de concrete eisen die voor een statistisch onderzoek gelden.

Voldoet de inrichting van het lab of de ontwikkeling van het (aan de slimme technologie ten grondslag liggende) algoritme niet aan deze vereisten, dan dient het onderzoek te voldoen aan reguliere eisen van de AVG.

Art. 89 AVG bepaalt dat ten behoeve van een statistisch onderzoek persoonsgegevens mogen worden verwerkt. Onder een onderzoek met een statistisch doeleinde wordt verstaan:

> "het verzamelen en verwerken van persoonsgegevens die nodig zijn voor statistische onderzoeken en voor het produceren van statistische resultaten. Die statistische resultaten kunnen ook voor andere doeleinden worden gebruikt, onder meer voor wetenschappelijke onderzoeksdoeleinden. Het statistische oogmerk betekent dat het resultaat van de verwerking voor statistische doeleinden niet uit persoonsgegevens, maar uit geaggregeerde gegevens bestaat, en dat dit resultaat en de persoonsgegevens niet worden gebruikt als ondersteunend materiaal voor maatregelen of beslissingen die een bepaalde natuurlijke persoon betreffen."[140]

Wij achten verdedigbaar dat het ontwikkelen van een algoritme ten behoeve van de slimme technologie op zichzelf gekwalificeerd kan worden als statistisch onderzoek, mits een heldere technische en organisatorische knip bestaat tussen de ontwikkeling van het algoritme. De wetgever heeft in de parlementaire geschiedenis onderkend dat het verwerken van persoonsgegevens ten behoeve van het ontwikkelen van een voorspellend risicomodel kan worden gezien als statistisch onderzoek.

> Zie Overweging 159 van de Preambule van de AVG, waarin wordt gesteld dat:
>
> "voor de toepassing van deze verordening de verwerking van persoonsgegevens met het oog op wetenschappelijk onderzoek ruim moet worden opgevat en bijvoorbeeld technologische ontwikkeling en demonstratie, fundamenteel onderzoek, toegepast onderzoek en uit particuliere middelen gefinancierd onderzoek omvatten".
>
> Zie *Kamerstukken II* 1998/99 25892, nr. 13, p. 8:

[140] Overweging 162 van de AVG.

"Is het onder de Wet bescherming persoonsgegevens mogelijk dat voor statistische doeleinden marktonderzoek wordt verricht, met de resultaten waarvan een sociale typografie van bijvoorbeeld een wijk wordt gemaakt?
(...)
Ja. Zolang het resultaat geen betrekking heeft op identificeerbare natuurlijke personen, is − ook al worden voor het verkrijgen van dat resultaat wel persoonsgegevens gebruikt − sprake van statistisch onderzoek. In dat geval is het soepeler regime van de wet van toepassing. Wij verwijzen naar art. 9, tweede lid, van het wetsvoorstel. Dit sluit aan bij de huidige praktijk."

Zie *Handelingen EK* 1999/00, 34-1623:

"Het tweede punt betreft de risicoanalyse. De toepassing van groepsprofielen op een individuele persoon betreft het gebruik van een persoonsgegeven en valt derhalve onder de werking van de wet. Het gebruik van persoonsgegevens voor de vervaardiging van groepsprofielen is een vorm van in het algemeen toelaatbaar geacht statistisch gebruik. Het groepsprofiel als zodanig valt evenwel buiten de werking van de wet (...). Denk bijvoorbeeld aan de constatering dat alle jongeren onder de 21 jaar een grotere kans op ongelukken maken.[141] Een ander voorbeeld is de verbinding van bepaalde postcodegroepen met bepaalde kenmerken. Voor het opstellen van groepsprofielen zijn vaak wel persoonsgegevens nodig. Art. 9, derde lid, duidt dit als een vorm van toelaatbaar verder gebruik van persoonsgegevens voor statistische doeleinden, mits toereikend is verzekerd dat de gegevens niet tevens voor andere doeleinden kunnen worden gebruikt. Wanneer het groepsprofiel evenwel wordt toegepast op een individuele persoon, gaat het wel weer om een persoonsgegeven[142]." (onderstreping toegevoegd)

Zie *Kamerstukken I* 1999-2000, 25892, nr. 92c, p. 13:

"Indien op grond van postcodesegmentatie of anderszins, bijvoorbeeld op grond van statistisch onderzoek, uit een bepaald gegeven dat aan iemands naam is toegevoegd, bepaalde gevolgtrekkingen worden gemaakt, gaat het om een persoonsgegeven. Het gegeven leidt er immers toe dat iemand in het maatschappelijk verkeer de kans loopt anders te worden bejegend dan wanneer dit gegeven niet over hem bekend was."

Om de verwerking ten behoeve van de ontwikkeling van het algoritme te kunnen baseren op artikel 89 AVG dient te worden voldaan aan de volgende randvoorwaarden:

(a) Het resultaat van het 'statistische onderzoek' bestaat slechts uit geaggregeerde − niet meer tot natuurlijke personen herleidbare − gegevens. Naar ons oordeel is goed verdedigbaar dat deze eis betekent dat het onderzoek *wel* zal mogen leiden tot algemene geaggregeerde, niet tot individuen herleidbare groepsprofielen/voorspelmodellen, die in zijn

[141] Vgl. ook Kamerstukken II 1997-1998, 25 892, nr. 3, p. 93: "Het derde lid is niet van toepassing indien het resultaat van de verwerking [lees, het statistisch onderzoek, adv.] niet op personen herleidbare informatie betreft. De statistische informatie mag in dat geval voor allerlei (andere) doeleinden worden gebruikt, dus bijvoorbeeld ook voor marketing-doeleinden (niet zijnde direct marketing)." In dat geval worden immers geen persoonsgegevens verwerkt.

[142] Dan worden immers persoonsgegevens verwerkt over degene op wie het profiel wordt toegepast.

algemeenheid kunnen worden toegepast ten behoeve van de slimme technologie.

(b) De geanalyseerde onderliggende persoonsgegevens worden niet gebruikt als ondersteunend materiaal voor individuele beslissingen.

(c) Er worden technische en organisatorische maatregelen getroffen om dit te verzekeren (functionele scheiding, anonimisering/pseudonimisering, verwijdering persoonsgegevens na afloop van het onderzoek).

Om te kunnen voldoen aan bovengenoemde voorwaarden dient de ontwikkelaar de volgende stappen te ondernemen:

- Controleer zekerheidshalve of de inrichting van de ontwikkelingomgeving en de onderzoeksopzet voldoet aan de hierna beschreven voorwaarden die aan een statistisch onderzoek worden gesteld.

- Tref technische en organisatorische maatregelen die borgen dat de onderliggende persoonsgegevens en het resultaat van de analyse niet (als ondersteunend materiaal) worden gebruikt om maatregelen en beslissingen te nemen die een specifiek natuurlijk persoon raken. Dit houdt onder meer het volgende in:

- Controleer of een functionele scheiding (‘*knip*’) is aangebracht tussen de ontwikkeling van het algoritme en de toepassing van het algoritme. Allereerst dient er een technische scheiding te worden aangebracht tussen enerzijds de ontwikkelomgeving en anderzijds de pilotomgeving (of omgeving waarbinnen het algoritme in productie is gebracht). Beide omgevingen moeten technisch en organisatorisch van elkaar zijn afgesloten.

- Zorg dat de pseudonimisering van de persoonsgegevens plaatsvindt in een afgeschermde omgeving waartoe enkel de daartoe bevoegde medewerker toegang heeft. Pas na het voltooien van het pseudonimiseringsproces mogen deze gegevens beschikbaar worden gemaakt in de ontwikkelomgeving.

- Borg − overeenkomstig het beveiligingsbeleid en het autorisatiebeleid − dat de medewerkers die betrokken zijn bij de ontwikkeling van het algoritme, géén rol hebben bij de pseudonimisering van de opgehaalde gegevens óf een toekomstige rol krijgen bij het uitvoeren van de toepassing van het algoritme of de slimme technologie in de pilot of de productieomgeving. Waarborg bovendien dat deze medewerkers geen toegang kunnen verkrijgen tot de pseudonimiseringsomgeving of de pilot- of productieomgeving (voor zover het gaat om dat specifieke algoritme).

- Borg dat de data scientist de nodige handelingen verricht om de noodzaak van de gegevens te borgen. Zorg er in ieder geval voor dat de dataset wordt gefilterd, zodat onnodige gegevens worden verwijderd. Detecteer en verwijder in de fase van 'preprocessing' de onjuiste en irrelevante gegevens.

- Borg in de fase van 'data preparation' door middel van filtering en preprocessing dat onnodige of overbodige gegevens worden verwijderd. Zorg er met name voor dat door middel van preprocessing (waar mogelijk) de gegevenssets worden teruggebracht tot een vereenvoudigde of geaggregeerde vorm, zodat de kans op individuele herleidbaarheid wordt verkleind.

- Bewaar van iedere iteratie van het algoritme een back-up van de gehanteerde persoonsgegevens en de uitkomsten van de toepassing van het algoritme in de pilot of de in het productie gebrachte algoritme, maar versleutel deze back-up en bewaar de back-up in een afgesloten omgeving. Voor zover mogelijk verdient het aanbeveling om deze versleuteling geautomatiseerd plaats te laten vinden. Draag het toegangsbeheer tot de afgesloten omgeving op aan een daartoe aangewezen persoon en stel een toegangsbeleid vast waarin is uitgewerkt in welke situaties de back-up mag worden ontsleuteld. Op deze wijze wordt de verwerking van deze persoonsgegevens beperkt tot het minimum.

- Als de ontwikkelaar de omgeving inricht op een wijze die voldoet aan de vereisten van artikel 89 AVG jo. artikel 9, tweede lid, aanhef en onder j, AVG jo. 24 UAVG mogen ook bijzondere persoonsgegevens worden verwerkt. In dat geval moet worden voldaan aan de volgende randvoorwaarden:

    - het onderzoek moet een algemeen belang dienen;
    - de verwerking van de bijzondere persoonsgegevens moet voor het statistisch onderzoek noodzakelijk zijn;
    - het vragen van uitdrukkelijke toestemming van de betrokkenen blijkt onmogelijk of kost onevenredige inspanning;
    - bij de uitvoering van het statistisch onderzoek is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer niet onevenredig wordt geschaad.

****

Bijlage 2

Sanctiekaart

Sanctiekaart

Belangrijkste mogelijkheden tot optreden bij discriminatoire of racistische spreekkoren - huidig recht (mei 2021)

Slachtoffer (speler/scheidsrechter/bevolkingsgroep)

Actie uit onrechtmatige daad (art. 6:162 BW) bij civiele rechter

Wat: mogelijkheid tot (beperkte) schadevergoeding, (bij herhaling) opleggen uitingsverbod en/of civiel stadionverbod

Wanneer: handelen in strijd met maatschappelijke zorgvuldigheid of inbreuk op bescherming eer en goede naam (art. 8 EVRM)

Optreden door individueel slachtoffer kan als belastend worden ervaren

Aangifte bij politie

a Groepsbelediging (art. 137c Sr)

Wanneer: bij opzettelijke belediging in het openbaar van een groep wegens o.a. ras (huidskleur, etniciteit)

Wie: ieder die kennis draagt van het feit; aangever hoeft niet tot de beledigde groep te behoren

b Eenvoudige belediging (art. 266 Sr)

Wanneer: bij belediging, mondeling of door feitelijkheden, van een persoon in het openbaar en in zijn tegenwoordigheid

Wie: het slachtoffer zelf, of een derde die is voorzien van een bijzondere schriftelijke volmacht van het slachtoffer; ook klacht (verzoek vervolging) van slachtoffer vereist

Club

Standaardvoorwaarden

Wat: verwijdering uit stadion, ongeldigverklaring toegangsbewijs, stadionverbod

Wanneer: (vermoeden van) voetbalgerelateerd wangedrag, gedrag dat het belang van voetbal kan schaden, een strafbaar feit of (anderszins) provocerend/bedreigend/beledigend gedrag (zie met name de artikelen 8.5 en 10 van de voorwaarden)

Eventueel aanvullende mogelijkheden of sancties op grond van eigen huisregels en/of huisregels stadion

Actie uit onrechtmatige daad (art. 6:162 BW) als werkgever namens de speler

Wat: mogelijkheid tot (beperkte) schadevergoeding, (bij herhaling) opleggen uitingsverbod en/of civiel stadionverbod

Wanneer: handelen in strijd met maatschappelijke zorgvuldigheid of inbreuk op bescherming eer en goede naam (art. 8 EVRM)

Aangifte bij politie

a Groepsbelediging (art. 137c Sr)

Wanneer: bij opzettelijke belediging in het openbaar van een groep wegens o.a. ras (huidskleur, etniciteit)

Wie: een vertegenwoordiger van de club

b Eenvoudige belediging (art. 266 Sr)

Wanneer: bij belediging, mondeling of door feitelijkheden, van een persoon in het openbaar en in zijn tegenwoordigheid

Wie: een vertegenwoordiger van de club, alleen met bijzondere schriftelijke volmacht van het slachtoffer; ook klacht vereist

KNVB

Standaardvoorwaarden

Wat: verwijdering uit stadion, ongeldigverklaring toegangsbewijs, stadionverbod, boete van 450,- per misdraging

Wanneer: (vermoeden van) voetbalgerelateerd wangedrag, gedrag dat het belang van voetbal kan schaden, een strafbaar feit of (anderszins) provocerend/bedreigend/beledigend gedrag (zie met name de artikelen 8.5 en 10 van de voorwaarden)

Actie uit onrechtmatige daad (art. 6:162 BW) bij civiele rechter

Mogelijkheid tot voeren van civiele procedure bij belediging van personen betrokken bij KNVB (scheidsrechters, grensrechters)

Wat: mogelijkheid tot (beperkte) schadevergoeding, (bij herhaling) opleggen uitingsverbod en/of civiel stadionverbod

Wanneer: handelen in strijd met maatschappelijke zorgvuldigheid of inbreuk op bescherming eer en goede naam (art. 8 EVRM)

Aangifte bij politie

a Groepsbelediging (art. 137c Sr)

Wanneer: bij opzettelijke belediging in het openbaar van een groep wegens o.a. ras (huidskleur, etniciteit)

Wie: een vertegenwoordiger van de KNVB

b Eenvoudige belediging (art. 266 Sr)

Wanneer: bij belediging, mondeling of door feitelijkheden, van een persoon in het openbaar en in zijn tegenwoordigheid

Wie: een vertegenwoordiger van de KNVB, alleen met bijzondere schriftelijke volmacht van het slachtoffer; ook klacht vereist

Bijlage 3

Casusposities

De BVO heeft ervoor gekozen om ter bestrijding van discriminatie en racisme binnen het voetbalstadion slimme camera's te plaatsen die op een geautomatiseerde wijze (potentiële) discriminerende of racistische gedragingen door toeschouwers herkent en registreert. De inzet van deze slimme technologie is gerechtvaardigd, omdat de voetbalclub − mede overeenkomstig de in dit rapport opgenomen keuzeladder − heeft gemotiveerd dat minder ingrijpende maatregelen geen uitkomst bieden (zie optie c van de keuzeladder signaleringsfase). De BVO heeft in overleg met de AP een vergunning aangevraagd voor het verwerken van eventuele strafrechtelijke persoonsgegevens die met de slimme technologie worden verwerkt.

Signaleringsfase

De veiligheidscoördinator stelt na afloop van de wedstrijd vast dat vijf personen op de tribune een racistisch spreekkoor inzetten. De veiligheidscoördinator stelt vast dat uit de geluidsfragmenten twee uitingen zijn af te leiden. Door inzet van slimme geluidsanalyse (in combinatie met technologie waarmee kan worden vastgesteld wie op dat moment de desbetreffende leus uitsprak) kan met voldoende zekerheid worden vastgesteld dat twee mannen de desbetreffende leuzen hebben geroepen. Zij maken zich schuldig aan twee vormen van racistisch gedrag:

- Ten eerste worden er uitingen gedaan over de huidskleur van een speler van de tegenpartij. Dit betreft racistisch gedrag gericht tot één specifiek persoon. De inschatting van de veiligheidscoördinator is dat deze uitingen vallen aan te merken als (individuele) belediging van de desbetreffende speler.
- Ten tweede stelt de veiligheidscoördinator vast dat de mannen racistische leuzen schreeuwen over een religieuze bevolkingsgroep. De veiligheidscoördinator vermoedt dat deze uitingen zijn aan te merken als groepsbelediging.

Aangezien de beelden aanleiding vormen voor nader onderzoek, slaat de veiligheidscoördinator de beelden en geluidsfragmenten (evenals het dossier met daarin de voorlopige bevindingen) op in de KVV.

Identificatiefase

Nadat de veiligheidscoördinator de twee vormen van racistisch gedrag (individuele belediging speler en groepsbelediging) heeft gesignaleerd, gaat de veiligheidscoördinator over tot een nadere analyse van de beelden. Het doel daarvan is het identificeren van de twee mannen. Bij veel voetbalclubs zal de identificatie handmatig gaan. De voetbalclub waar de veiligheidscoördinator werkzaam is heeft echter recentelijk − overeenkomstig de keuzeladder identificatiefase − ervoor gekozen om de kaartverkoop te koppelen aan een preregistratie van de koper van het ticket. Bij de toegangscontrole wordt geregistreerd wanneer de houder van het ticket het stadion is binnengekomen, inclusief zijn toegewezen zitplaats.

De veiligheidscoördinator stelt bij de analyse − door middel van een locatiesoftware van de slimme camera − vast dat de twee mannen zich bevonden op stoelnummer 15 (man 1) en 16 (man 2), vak D. Man 1 blijkt een seizoenkaarthouder te zijn. De veiligheidscoördinator stelt de identiteit van man 1 als volgt vast:

- aan de hand van de toegangspoortregistratie checkt de veiligheidscoördinator wie op stoel 15 is geregistreerd;
- de persoonsgegevens behorend bij stoel 15 zijn gekoppeld aan een seizoenskaart;
- aangezien seizoenkaarthouders reeds een foto hebben moeten inleveren ten behoeve van de seizoenkaart, kan de veiligheidscoördinator de identiteit van man 1 vaststellen. De ingeleverde foto komt overeen met de vastgelegde beelden tijdens de wedstrijd.

Man 2 is daarentegen geen seizoenkaarthouder. De identiteit van man 2 wordt als volgt vastgesteld:

- de veiligheidscoördinator stelt aan de hand van de preregistratie de naam en het adres vast van degene die op stoel 16 is geregistreerd;
- ook kan de veiligheidscoördinator vaststellen dat degene die op stoel 16 is geregistreerd om 14:30 door toegangspoort 3 het voetbalstadion is binnengekomen;
- de veiligheidscoördinator stelt aan de hand van de bewakingsbeelden op dat tijdstip van toegangspoort 3 vast dat degene die op stoel 16 is geregistreerd man 2 is.

Nu beide mannen zijn geïdentificeerd, komt daarmee de identificatiefase ten einde.

Sanctiefase

De KNVB besluit allereerst civielrechtelijk op te treden tegen de twee mannen. Het doel is met name het opleggen van een landelijk stadionverbod. Daarnaast doet de BVO aangifte bij de politie tegen beide vormen van racistisch gedrag. De getroffen speler besluit evenwel af te zien van het doen van aangifte.

Civielrechtelijk optreden

Zoals volgt uit de sanctiekaart heeft de KNVB verschillende opties om de twee mannen civielrechtelijk aan te spreken. De KNVB standaardvoorwaarden, die door clubs bij de in artikel 1 onder f van die standaardvoorwaarden bedoelde voetbalwedstrijden van toepassing verklaard dienen te worden, spelen bij deze sanctieoplegging (zowel voor de clubs als voor de KNVB) een sleutelrol. In aanvulling daarop kunnen clubs zich bij het opleggen van sancties ook baseren op de rechten die zij ontlenen aan het feit dat zij eigenaar of huurder zijn van het stadion waarin zij spelen. Artikel 8.5 van de KNVB

standaardvoorwaarden verbiedt (onder andere) gedrag dat als beledigend kan worden ervaren:

> "8.5 Het is verboden zich in het Stadion te gedragen op een wijze die anderen als provocerend, bedreigend of beledigend kunnen ervaren. […]."

Artikel 10 van de KNVB standaardvoorwaarden kent clubs en de KNVB vervolgens het recht toe bij overtreding van deze (of andere) bepaling(en) verschillende sancties op te leggen, waaronder onmiddellijke verwijdering uit het stadion, ongeldigverklaring van het toegangsbewijs, of – met inachtneming van de Richtlijn termijn stadionverbod - de oplegging van een (landelijk) stadionverbod.

In aanvulling op de verbintenisrechtelijke sanctiemogelijkheden die de standaardvoorwaarden de KNVB en clubs toekennen, wijzen wij (omwille van de volledigheid) op de aanvullende mogelijkheid om, desgewenst, ook buiten de KNVB standaardvoorwaarden om civielrechtelijk tegen verspreiders van racistische en discriminatoire uitlatingen op te treden. Dat kan op basis van artikel 6:162 van het Burgerlijke Wetboek, op grond waarvan, anders dan het geval is bij de KNVB standaardvoorwaarden, ook de slachtoffers van discriminatoire of racistische uitingen zelf de mogelijkheid hebben in rechte tegen de verspreiders van die uitingen op te treden.

Het door de slimme technologie verzamelde bewijsmateriaal (signalering en identificatie van de daders) zal in het kader van de civielrechtelijke procedure als bewijs mogen worden ingebracht. Eventuele bijzondere en strafrechtelijke persoonsgegevens op de beelden (bijvoorbeeld de van de beelden af te lezen indirecte rasgegevens van beide mannen die ten behoeve van identificatie zijn verwerkt) mogen ten behoeve van de procedure worden verstrekt, mits er daadwerkelijk één van de in de sanctiekaart genoemde (rechts)middelen is ingezet en de verwerking van deze gegevens strikt noodzakelijk zijn voor de instelling, uitoefening of onderbouwing van een rechtsvordering (zie artikel 22, tweede lid, aanhef en onder e, UAVG jo. artikel 32, aanhef en onder d, UAVG). Deze noodzaak kan worden aangenomen als de beelden strikt noodzakelijk zijn voor de bewijsvoering.

Tijdens de procedure wordt door de KNVB vastgesteld dat op basis van het bestaande materiaal niet goed kan worden vastgesteld of man 2 zich schuldig maakt aan individuele belediging van de speler. De KNVB wijst een deskundige aan die door middel van een nadere analyse de bewijswaarde van de beelden of geluidsfragmenten poogt te verbeteren. Concreet krijgt deze deskundige de opdracht om vast te stellen of man 2 degene is die de individuele uiting heeft geroepen. Mits noodzakelijk voor de analyse, is het verdedigbaar dat daarbij bijzondere en/of strafrechtelijke persoonsgegevens worden verwerkt. De verwerking daarvan kan dan gebaseerd worden op artikel 22, tweede lid, aanhef en onder e, UAVG respectievelijk artikel 32, aanhef en onder d, UAVG. Er is immers één van de in de sanctiekaart genoemde (rechts)middelen ingezet en de verwerking van deze gegevens is strikt noodzakelijk

voor de instelling, uitoefening of onderbouwing van een rechtsvordering. Op basis hiervan mogen dan ook biometrische gegevens worden verwerkt.

De deskundige in deze zaak stelt na inzet van gezichtsherkenningstechnologie vast dat man 2 de individuele uiting heeft geroepen.

Uitkomst van de procedure is dat voor beide mannen een stadionverbod wordt opgelegd.

Strafrechtelijk optreden

Zoals eerder toegelicht, doet de BVO aangifte bij de politie tegen beide vormen van racistisch geweld. De getroffen speler besluit evenwel af te zien van het doen van aangifte.

Zoals volgt uit de sanctiekaart kan de BVO aangifte doen voor groepsbelediging. De politie kan deze aangifte in behandeling nemen. Groepsbelediging (strafbaar gesteld in artikel 137c Wetboek van Strafrecht ('Sr')) betreft het zich in het openbaar opzettelijk beledigend uitlaten over een groep mensen, wegens onder meer hun ras. 'Ras' wordt ruim opgevat en betreft huidskleur, nationaliteit en etniciteit. Groepsbelediging is dus niet het beledigen van iemand *door* een groep, maar het beledigen door één of meer personen *van* een groep. 'Belediging' heeft de strekking een ander c.q. een groep bij het publiek in een ongunstig daglicht te stellen en in zijn eer of goede naam aan te tasten. Voor het bewijs van groepsbelediging is het niet vereist dat onder het publiek mensen aanwezig zijn van (bijvoorbeeld) joodse afkomst of met een donkere huidskleur. Het gaat erom dat de belediging publiekelijk is gehoord en gevoelens van vernedering of geschoktheid teweeg heeft kunnen brengen. Zie Hoge Raad 15 september 2009, ECLI:NL:HR:2009:BI4739, rov. 2.2.3.

De officier van justitie zal de rechtmatige (door middel van de slimme technologie vastgelegde) beelden met een beroep op Artikel 126nd Wetboek van Strafvordering ('Sv') kunnen vorderen bij de BVO. Artikel 126nd Sv bepaalt dat in geval van een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv de officier van justitie in het belang van het onderzoek van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens kan vorderen deze gegevens te verstrekken. Onder de misdrijven als bedoeld in artikel 67, eerste lid, Sv valt onder meer het misdrijf van artikel 137c Sr: *Hij die zich in het openbaar, mondeling (…) opzettelijk beledigend uitlaat over een groep mensen wegens hun ras (…) wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.*

De club die de camerabeelden heeft gemaakt van mogelijk strafbare gedragingen geldt als 'degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot vastgelegde gegevens' als bedoeld in artikel 126nd Sv. Aan de vordering van de officier van justitie dient te worden voldaan. Er is sprake van een wettelijke

verplichting tot het verstrekken van persoonsgegevens (artikel 6, eerste lid, aanhef en onder c, AVG).

Hoewel dit niet expliciet wordt opgemerkt in de aangiftebevoegdheid van artikel 161 Sv, is goed verdedigbaar dat de BVO bij de aangifte de beelden verstrekt met daarop strafrechtelijke gegevens. Een aangifte heeft immers per definitie betrekking op een (vermeend) strafbaar feit. In zoverre is artikel 161 Sv een lidstatelijke bepaling als bedoeld in artikel 10 AVG. De verwerking van bijzondere persoonsgegevens in de aangifte kan vervolgens worden gebaseerd op artikel 23, aanhef en onder c, UAVG dat bepaalt dat bijzondere persoonsgegevens (voor zover noodzakelijk) in aanvulling op strafrechtelijke persoonsgegevens mogen worden verwerkt.

Zodra de politie respectievelijk het OM de beelden hebben ontvangen, valt de verwerking van de daarin opgenomen persoonsgegevens niet langer onder de reikwijdte van de AVG. Vanaf dat moment is de Wpg respectievelijk de Wjsg van toepassing op de verwerking van de (bijzondere en/of strafrechtelijke) persoonsgegevens.

De rechter bepaalt vervolgens of de beelden toelaatbaar zijn als bewijs. De verwachting is dat de beelden als bewijsmateriaal zullen mogen worden gebruikt, voor zover de voetbalclub bij de inzet van de slimme technologie zich heeft gehouden aan de in dit rapport beschreven randvoorwaarden.

De politie kan de aangifte van de BVO gericht tegen de eenvoudige (individuele) belediging van de speler van de tegenpartij niet in behandeling nemen. Daarvoor is vereist dat het slachtoffer zelf aangifte doet of de BVO daarvoor volmachtigt. Aanvullend geldt dat het slachtoffer daadwerkelijk een klacht moet indienen. Doordat de speler dit niet heeft gedaan, kan de strafrechtelijke vervolging geen doorgang vinden. Het is de BVO niet toegestaan om de beelden en het dossier (incl. de daarin opgenomen strafrechtelijke en mogelijk zelfs bijzondere persoonsgegevens) aan de politie te verstrekken. Nu geen onderzoek mogelijk is, kan een dergelijke verstrekking niet noodzakelijk worden geacht. Daarmee eindigt de sanctiefase.

****